Data Classification - Procedures

APPROVAL AUTHORITY

Chief Operating Officer

RESPONSIBLE EXECUTIVE MEMBER

Chief Operating Officer

DESIGNATED OFFICER

Chief Data Officer

FIRST APPROVED

3 December 2024

LAST AMENDED

3 December 2024

REVIEW DATE

3 December 2026

STATUS

Active

1. Purpose

1.1 These procedures provide a structured approach to applying classifications to data and information assets to support confidentiality, security, and privacy considerations.

1.2 These procedures must be read in conjunction with the linked Data Governance – Operational Policy, and Data Handling – Guidelines (login required).

2. Scope and application

2.1 These procedures apply to all University staff, students undertaking research or involved in other University business, approved third parties, alumni, contractors, and sub-contractors. It includes all individuals who handle University data and information, regardless of their role or affiliation.

2.2 These procedures apply to all University data and information.

3. Definitions

3.1 Refer to the University's Glossary of Terms for definitions as they specifically relate to policy documents.

3.2 The terms data and information are used interchangeably within these procedures, recognising the overlap between the two. In their simplest form, data is often considered as raw values and individual facts in any form, and information is data that has been contextualised. Both data and information can be University records.

4. Data classification

4.1 Data classification refers to the application of a classification level to data and information that controls its intended audience with respect to the privacy, confidentiality, and business criticality.

4.2 Data users who capture data and information must assess the nature of the content with consideration to the confidentiality, privacy, and potential impact of unintentional disclosure or loss, to determine the classification. The Data Custodians are accountable for ensuring all data and information within their data domain is classified appropriately.

4.3 The classification applied informs technical and handling controls required for the data or information and must be actioned in accordance with the Data Handling – Guidelines (login required).

4.4 Confidentiality Integrity Availability (CIA) triad

4.4.1 Classification levels are contextualised by the Confidentiality, Integrity and Availability (CIA) triad, a universally recognised model for information security.

4.4.2 When determining the appropriate classification for data and information, the following parameters must be considered:

(a) Confidentiality: ensuring the appropriate level of access or restrictions that need applying to data and information, based on the sensitivity of the content;

(b) Integrity: ensuring that data and information is created, amended, or deleted only by the appropriate persons, providing assurance that it is accurate, reliable and can be trusted; and

(c) Availability:ensuring data and information is available when it is needed and by the intended authorised users, with consideration to the consequences of not having access to the data when required.

4.5 Risk management

4.5.1 Data classification takes into consideration the impact on the University should data or information be unintentionally disclosed, altered, interfered with, lost or destroyed without authorisation. Consideration of data-related risks must be in accordance with the Risk Management - Governing Policy.

4.6 Data classification levels

4.6.1 All University data must have one of 6 classification levels applied:

(a) UNOFFICIAL;

(b) PUBLIC;

(c) INTERNAL – STAFF;

(d) INTERNAL – STAFF AND STUDENTS;

(e) SENSITIVE; or

(f) RESTRICTED.

4.6.2 The default classification is INTERNAL - STAFF. Data and information that has not been specifically classified is deemed INTERNAL - STAFF.

4.6.3 Classification levels must be applied at the data asset level where practicable. For documents, this is at the individual document level.

4.6.4 When varying classification levels are identified for collections of data (e.g., within business systems), they must be classified as a whole, with the highest classification level applied. Table 1: Data classification level descriptions illustrates the classification level and their descriptions.

Table 1: Data classification level descriptions

CLASSIFICATION NAME	DESCRIPTION	EXAMPLES CAN INCLUDE
UNOFFICIAL	Data and information not relevant to official University business. This includes personal or non-work-related data that has been captured using university resources. Limited personal use of University ICT resources must be in accordance with the Acceptable Use of ICT Resources - Operational Policy.	- Personal emails - Casual notes - Industry newsletter
PUBLIC	Data and information created for public dissemination with no confidential content. This type of information being in the public domain, would have no impact on the university.	- Websites - Digital media - Media releases - Course catalogues - Annual reports - Open access research publications
INTERNAL – STAFF AND STUDENTS	Data and information intended only for university staff, Higher degree by research (HDR) students, and approved third parties, contractors, sub-contractors, and any other person who undertakes university business, as well as UniSC students. If this data is inappropriately disclosed, lost or destroyed, this may have a mild impact on the university and/or its stakeholders.	- Internal student newsletters - Course curriculum content - Student services information
INTERNAL - STAFF	Data and information intended only for university staff, Higher degree by research (HDR) students, and approved third parties, contractors, sub-contractors, and any other person who undertakes university business.	- Business process documents - Meeting minutes - Reports

	The INTERNAL – STAFF label is the University's default label, and must be upgraded or downgraded as appropriate. If this data is inappropriately disclosed, lost or destroyed, this may have a mild impact on the university and/or its stakeholders.	
SENSITIVE	Data and information available only to university staff and HDR students within approved business groups or approved third parties, contractors, sub-contractors, and any other person who undertakes university business that have a legitimate need for access, given confidentiality and privacy. University groups may include specified business areas, working groups, committees, or project teams. If this data is inappropriately disclosed, lost or destroyed, it would have a significant impact on the university and/or its stakeholders. All research data must have a minimum classification of SENSITIVE. The classification level can be downgraded when research outputs (including publications and datasets) have been published.	- Student personal data - Employee personal data - Confidential project details - University budgets - Research data
RESTRICTED	Restricted data and information must be classified for access by named individuals only, due to privacy and confidentiality. If this data is inappropriately disclosed, lost or destroyed, it would have a critical impact on the university and/or its stakeholders. This data has the strictest levels of access and security controls applied to prevent unauthorised disclosure, loss, destruction or theft.	- Medical health records - Identity documents - Financial information, including credit card, banking details or tax file numbers - Commercial-in-confidence research

4.7 Data handling

4.7.1 The application of data classifications and association must be applied in accordance with the Data Handling – Guidelines (login required).

4.8 Alternative data classifications and controls

4.8.1 In exceptional circumstances, additional or alternate data classifications and controls can be applied to data and information relevant to a contract or agreement for a defined activity or project. Examples can include research projects which require adherence to Defence Industry Security Program (DISP) standards.

4.8.2 These can only be applied with the approval of the Chief Data Officer.

5. Monitoring and reporting

5.1 Regular monitoring and reporting on the application of data classification procedures is reported to the Data Analytics and Information Management Advisory Committee.

5.2 The Chief Data Officer monitors and reports on University compliance with these procedures in accordance with the Compliance Management Framework - Governing Policy.

6. Authorities and responsibilities

6.1 As the Approval Authority the Chief Operating Officer approves these procedures to operationalise the Data Governance – Operational Policy.

6.2 As the Responsible Executive Member the Chief Operating Officer can approve guidelines to further support the operationalisation of these procedures. All procedures and guidelines must be compatible with the provisions of the policy they operationalise.

6.3 As the Designated Officer of these procedures the Chief Data Officer is authorised to approve associated documents to support the application of these procedures.

6.4 These procedures operate from the last amended date, with all previous procedures related to the data classification replaced and have no further operation from this date.

6.5 All records relating to data classification must be stored and managed in accordance with the Records Management - Procedures.

6.6 These procedures must be maintained in accordance with the Policy Framework – Procedures and reviewed on the shortened 2-year policy review cycle.

6.7 Any exception to this policy to enable a more appropriate result must be approved in accordance with the Policy Framework – Procedures prior to any deviation from these procedures.

6.8 Refer to Schedule C of the Delegations Manualin relation to the approved delegations detailed within these procedures.

6.9 Data Classification Roles

6.9.1 The following roles, responsibilities and accountabilities are specific to these procedures and cascade from the high-level roles and responsibilities in the Data Governance – Operational Policy.

ROLE	POSITION	RESPONSIBILITY AND ACCOUNTABILITY
Chief Data Officer	Chief Data Officer	Accountable for: (a) implementation, adoption and continuous monitoring of data classifications throughout the data lifecycle; and (b) risk assurance for data classification application. Responsible for: (a) embedding data classifications into university data governance processes and business systems, and ensuring their ongoing application and regular reviews of classification levels; (b) implementing stringent data handling controls and ensuring their maintenance; (c) appointing and inducting Data Custodians; and (d) ensuring high levels of guidance and support for Data Custodians and Data Users for data classification implementation and maintenance.
Data Custodians	Heads of Departments (appointed by CDO)	Accountable for: (within their data domain) (a) ensuring data within their Data Domain (in accordance with the Data Governance – Operational Policy) is appropriately classified. Responsible for: (a) establishing and embedding local Domain-specific processes for data classification, and ensuring the provision of guidance on their application as relevant to their Data Domain; (b) identifying and addressing Data Domain specific risks or requirements related to data classification, including the implications of classification decisions; (c) considering data classifications when approving data sharing and access requests; (d) Nomination of subject matter experts and ongoing support for their role; and (e) providing support to Data Users for the use of data classification levels.
Business System Owners	In accordance with the ICT Security - Operational Policy	Responsible for: (a) ensuring classification labelling functionality is enabled within their system, where applicable; (b) identifying the types of data held in their respective system and the application of appropriate data classifications;

		(c) monitoring and reviewing the application of technical system controls to secure data based on the highest level of classification applicable; (d) adjusting technical and security controls in response to changes in data classifications; and (e) managing access controls in accordance with data classification levels within the system.
Data Subject Matter Experts	Staff based on specific expertise-criteria relative to a data asset	Responsible for: (a) advising on appropriate classifications for data assets in their area of expertise; and (b) providing guidance to data users on applying classification levels.
Data Users	All University staff, affiliates and/or groups that create or use data	Responsible for: (a) applying and maintaining data classifications; (b) reporting any classification discrepancies or security concerns to the appropriate Data Custodian; and (c) adhering to these procedures and the Data Handling – Guidelines (login required).

END

RELATED DOCUMENTS

- Acceptable Use of ICT Resources - Operational Policy

- Compliance Management Framework - Governing Policy
- Compliance Management Framework - Procedures
- Data Management - Procedures
- ICT Security - Operational Policy
- Records Management - Procedures

LINKED DOCUMENTS

- Data Governance - Operational Policy

RELATED LEGISLATION / STANDARDS

- Right to Information Act 2009 (Qld)
- Public Records Act 2023 (Qld)
- Information Privacy Act 2009 (Qld)