Information Asset and Security Classification Procedure

1 Purpose

To establish a process for classifying and managing University Information Assets based on their sensitivity, value and criticality. This Procedure outlines the actions required to ensure compliance with the ICT Information Management and Security Policy.

2 Scope

This Procedure applies to all Universities Information Assets, including those collected, created, handled, or stored by the University. It also applies to all Users who access, process, store, or share University Information.

3 Procedure Overview

This Procedure outlines the framework for classifying and managing Information Assets by specifying accountabilities and responsibilities at different stages of the information lifecycle, applying security controls, maintaining audit logs, and retention and disposal requirements.

This procedure aligns with:

- Higher Education Standards Framework (Threshold Standards) 2021: Standard 7.3 Information Management.
- Higher Education Support Act (2003):
    - Division 179-Protection of Personal Information and
    - Division 180-Disclosure or Use of Higher Education Support Act Information

4 Procedures

4.1 Information Asset and Security Classification framework

Information Assets are classified based on their security levels to help protect their confidentiality, integrity and availability. Classifications further indicate the level of impact to the University should that information be compromised, disclosed, altered, or destroyed without authorisation.

Baseline Security Controls are further applied to Information Assets to help safeguard them from unauthorised access by specifying data access rights that may be assigned to Users. By default, all University Information Assets are classified as Official unless otherwise re-assigned by this Procedure, as listed in Table 1, or by Information Systems Custodian or Data Custodians using the steps outlined in the Information Asset and Security Classification Schedule.

For Information Assets without Security Classifications, the Information System Custodian or Data Custodian must refer to the Data Types listed in Table 1 and consult the Information Asset and Security Classification Schedule to determine whether the asset requires a reclassification. Externally generated assets that have not been classified must be reviewed by the receiving University officer, in consultation with the Information System Custodian or Data Custodian.

University Information Assets are classified into four sensitivity classifications:

Table 1. Information Classifications

Classification	Access	Description	Examples
Tier 1: Public	No access approvals required	Public Information Assets can be shared openly with anyone.	• University Organisational information, including Strategic Plans, Annual reports, organisational charts, Campus maps and buildings • Policy Instruments • Curriculum outlines of programs, study components, and courses • Academic Calendar • Types of Supports for Students, supports for learning and teaching • Results collected from evaluations or academic or institutional research collected anonymously or reported in aggregated formats • Research profiles, opportunities, outcomes, and impact

			• Affiliations and partnerships with external organisations
Tier 2: Official	University Employees are provided default access. Persons of Interest, contractors and affiliates must obtain approval from relevant Custodians.	Official Information Assets relate to official University business and may be distributed internally or externally. These datasets may be used for reporting to State and Federal Governments or other regulatory or authoritative bodies. Datasets are made available to all Employees, and may be published in aggregated formats on UniSQ websites, subject to relevant approvals.	• Information collected from students, including contact details (name, address, phone, personal email) required for regulatory reporting • Administrative Student, Employee and academic and institutional research management data • National and institutional data collections, including Tertiary Collection of Student Information (TCSI) datasets, Student evaluation administration data and responses (QILT, Student Course Feedback Surveys)
Tier 3: Confidential	Only accessible by University Employees with delegated data access rights as authorised by Data and Systems Custodians. Refer to Table 1 in the Information Asset & Security Classification Schedule.	Confidential Information Assets contain personal or financial data.	• Student and Employee personal details, including bank accounts, passport details • Individual response identifiers in survey responses (QILT, Student Course Feedback Surveys) • Employees and third-party contracts • Cyber and physical security reports • Financial forecast, and

			• University sales and procurements account data
Tier 4: Restricted	Only accessible to University Employees when access is granted by University Senior Executives.	Restricted Information Assets are highly sensitive and can cause damage if disclosed without authorisation and are not to be shared internally or externally (unless otherwise approved by University Senior Executives)	• Student and Employee, Government, health or equity information, including Tax File Numbers, health records, medical consultations and certificates, Low Socio-Economic Statuses, disability support details • Grievances, Appeals and Complaints • Financial account details, entitlements, supports, and payment records • Intellectually sensitive business data, research, or source codes

These classifications are assigned across the University within the UniSQ Data Reference Model, accessible to all Employees via the UniSQ Enterprise Information Management SharePoint site.

Note: All Information maintained by the University are subject to third party legal discovery such as subpoenas and Right to Information access requests which are processed by Enterprise Information Management Services.

4.2 Accountabilities and responsibilities

All University Employees, including Person of Interest, contractors, and affiliates, with access granted to University data, are required to adhere to implemented controls.

4.2.1 Information Systems and Information Assets

1. Each Information Systems and Information Assets are uniquely identified, assigned a Custodian and given an Information Classification, if not already classified.

2. Refer to the Information Asset and Security Classification Schedule for guidance on classification processes, including identification of Custodians (Table 1),additional

responsibilities (Table 2), and associated risks and safeguards (Tables 3 and 4)

4.2.2 Custodian Responsibilities

1. Information System Custodian or Data Custodian must ensure that Employees are trained in the effective use of the relevant Information System and associated Information Assets.

2. Custodians are responsible for implementing appropriate controls for monitoring their systems or assets, authorising and revoking access for Confidential or Restricted Information Systems, and addressing identified audit issues with ICT Services' assistance.

4.2.3 ICT Services Responsibilities

1. Monitor the University's ICT network infrastructure, including all hardware and communications links, and support and address audit issues

2. Support Information Systems Custodians to manage the information lifecycle for data integrated or exported to the University's enterprise information, data and analytics infrastructure, as outlined by the ICT Information Management and Security Policy.

3. Monitor and assist Custodians with compliance obligations in accordance with impact assessment guidance listed in Table 3 of the Information Asset and Security Classification Schedule.

4. Provide secure access through a central authentication system, including provision of usernames and passwords to access the University's network.

4.2.4 Data Access and Usage

1. All University Employees are required to complete the Data Access Agreement and must ensure that Information Assets are handled using UniSQ provisioned ICT software and hardware with UniSQ provisioned Virtual Private Network (VPN) enabled using Multi-Factor Authentication (MFA).

2. Confidential or Restricted information may only be collected or accessed when required to do so for University business.

3. Confidential or Restricted information must be de-identified before sharing or disclosing, except when reported to Government.

4.2.5 First Nations Data Handling

1. Research data must be handled in accordance with the AIATSIS code of Ethics for Aboriginal and Torres Strait Islander Research.

2. Administrative Student and Employee data for First Nations peoples must be handled in accordance with the Indigenous Data Sovereignty guidelines outlined by Maiam Nayri Wingara.

4.3 Applications of Security Controls

Security controls must be applied to protect Information Assets at all stages of the Information Asset lifecycle. Unlike a risk assessment, data security classifications have been determined by the potential level of impact to the organisation or individual should the data be shared inappropriately or compromised (for Information Assets requiring reclassification, refer to Table 3 in the Information Asset and Security Classification Schedule).

The Information System Custodian must ensure that these controls are in place by following:

1. **Applying the Need-to-Know Principle:** Confidential and Restricted Information Assets should only be accessible to individuals who require them for their work duties.

2. **Implementing a Clear Desk Policy:** Official, Confidential, and Restricted Information Assets must be secured in accordance with advice outlined in the Information Asset and Security Classification Schedule to prevent unauthorised access to any electronic materials or systems.

3. **Handling Security Classified Information Assets from external organisations:** Retain the security classification as received from the data transfer. Manage the assets according to the University's Confidentiality Agreement with the external organisation, ensuring the originator of the data transfer is responsible for its protection.

4. **Referencing Safeguarding Measures:** Consult Table 4 of the Information Asset and Security Classification Schedule for detailed safeguarding measures specific to each classification.

4.4 Audit Logs

With security controls applied, a strict audit logging process must be implemented to track and maintain the confidentiality and integrity of Information Assets. The audit logs provide a trail of evidence for investigations and must be protected with access controls, as outlined in the Information Asset and Security Classification Schedule (Table 4).

4.5 Retention and Disposal of Information Assets

To ensure ongoing compliance, the retention and disposal of Information Assets must follow the

security classifications and legal requirements set out in the Information Asset and Security Classification Schedule (Table 4), which adheres to the University's obligations as outlined by the Queensland General Retention and Disposal Schedule.

4.6 Information Asset Register

All classified Information Assets must be recorded in the Information Asset Register. The University provides public access to this register in line with Queensland and National legislative requirements, supporting transparency and accountability as outlined by the Right to Information Policy.

Information held by the University, including the Information Asset Register, may be sought through the University's Administrative Access Scheme, Publication Scheme, Disclosure Log or a formal access request under the *Right to Information Act 2009* or *Information Privacy Act 2009* which are available on the Right to Information and Privacy websites.

The Information System Custodian must ensure that the Information Asset Register is reviewed, updated, and maintained annually. This process ensures that all assets are accounted for and properly classified. ICT Services will assist as necessary to support this ongoing responsibility.

4.7 Non-Compliance

Failure to adhere to the procedures outlined in this document may result in disciplinary actions in accordance with the University's Policy Instruments.

5 References

Australian Institute of Aboriginal and Torres Strait Islander Studies. *AIATSIS code of Ethics for Aboriginal and Torres Strait Islander Research*. Retrieved June 2024 from https://aiatsis.gov.au/sites/default/files/2020-10/aiatsis-code-ethics.pdf

The Australian Indigenous Data Sovereignty Collective. *Maiam Nayri Wingara*. Retrieved June 2024 from https://www.maiamnayriwingara.org/

6 Schedules

This procedure must be read in conjunction with its subordinate schedules as provided in the table below.

7 Procedure Information

Accountable Officer	Chief Information Officer
Responsible Officer	Chief Information Officer

Policy Type	University Procedure
Policy Suite	ICT Information Management and Security Policy
Subordinate Schedules	Information Asset and Security Classification Schedule
Approved Date	24/1/2025
Effective Date	24/1/2025
Review Date	24/1/2030
Relevant Legislation	AS ISO/IEC 27000:2018 - Security technology-Security techniques-Information security management systems-Overview and vocabulary AS ISO/IEC 27001: 2022 - Information security, cybersecurity and privacy protection-Information security management systems-Requirements AS ISO/IEC 27002: 2022 - Information security, cybersecurity and privacy protection-Information security controls AS ISO/IEC 27005: 2022 - Information security, cybersecurity and privacy protection-Guidance on managing information security risks *Electronic Transactions (Queensland) Act 2001* *Information Privacy Act 2009* Information Security Manual - ISM (Australian Government) *Integrity Act 2009* Metadata Management Principles *Public Interest Disclosure Act 2010* (Qld) *Public Records Act 2023* *Public Sector Ethics Act 1994* Queensland Government Information Security Classification Framework Queensland Information Standard 02: ICT Resources Strategic Planning Queensland Information Standard 13: ICT Procurement and Disposal of ICT Products and Services

	Queensland Information Standard 18: Information Security Queensland Information Standard 31: General Retention and Disposal Queensland Information Standard 33: Information Access and Use Queensland Information Standard 38: Use of ICT Facilities and Devices Queensland Information Standard 39: Domain Names Queensland Information Standard 44: Information Asset Custodianship Records Governance Policy *Right to Information Act 2009* *University of Southern Queensland Act 1998*
Policy Exceptions	Policy Exceptions Register
Related Policies	Acceptable use of ICT Resources Policy Code of Conduct Policy Delegations Policy Enterprise Risk Management Policy Fraud and Corruption Management Policy Privacy Policy Public Interest Disclosure Policy Records and Information Management Policy Right to Information Policy Student Communication Policy
Related Procedures	Privacy Procedure Research Data and Primary Materials Management Procedure Student Communication Procedure Use of Electronic Mail Procedure

Related forms, publications and websites	Enterprise Information Management Framework (EIM Framework) Internal Information Asset Register External Information Asset Register UniSQ Data Reference Model ServiceHub - Data Access Agreement Disposal Schedules Records Disposal Register Form Right to Information website Privacy website
Definitions	**Terms defined in the Definitions Dictionary**
	Employee A person employed by the University and whose conditions of employment are covered by the Enterprise Agreement and includes persons employed on a continuing, fixed term or casual basis. Employees also include senior Employees whose conditions of employment are covered by a written agreement or contract with the University. Information Any collection of data that is processed, analysed, interpreted, organised, classified or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form. Information Asset An identifiable collection of data stored in any form and recognised as having value for the purpose of enabling the University to perform its business functions, thereby satisfying a recognised University requirement. Information Classification Classified data represents data classified as either Public Information, Internal Information or Restricted Information in this document. The

classification of an Information Asset is to identify Security Controls required to protect that asset.

Information Security

Concerned with the protection of Information from unauthorised use or accidental modification, loss or release.

Information System Custodian

An individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a System within the University.

Information Systems

The organised collections of hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information.

Internal Information

Information should be classified as Internal when the unauthorised disclosure, alteration, or destruction of that Information could result in a moderate level of risk to the University. By default, all Information Assets that are not explicitly classified as Restricted Information or Public Information should be treated as Internal Information. A reasonable level of Security Controls should be applied to Internal Information. Access to Internal Information must be requested from, and authorised by, the Information System Custodian. Access to Internal Information may be authorised to groups of persons by their job classification or responsibilities (e.g. role-based access). Internal Information is moderately sensitive in nature. Often Internal Information is used in making decisions, and therefore it is important this information remain timely and accurate. The risk for negative impact on the University should this information not be available when needed is moderate.

Personal Information

Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion - (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.

Public Information

Information should be classified as Public when the unauthorised disclosure, alteration, or destruction of that Information would result in little or no risk to the University. While little or no controls are required to protect the confidentiality of Public Information, some level of control is required to prevent unauthorised modification or destruction of that Information. Public Information is not considered sensitive; therefore, it may be granted to any requestor or published with no restrictions. The integrity of Public Information should be protected and in particular, the growing social media phenomenon casts doubts on the messages contained within. The appropriate Information System Custodian must authorise replication or copying of the Information in order to ensure it remains accurate over time. The impact on the University should Public Information not be available is low.

Restricted Information

Information should be classified as Restricted when the unauthorised disclosure, alteration, or destruction of that Information could cause a significant level of risk to the University or its affiliates. Restricted Information includes Information protected by the State or Commonwealth privacy regulations and Information protected by confidentiality agreements. The highest level of Security Controls should be applied. Access to Restricted Information must be controlled from creation to destruction, and will be granted only to those persons affiliated with the University who require such access in order to perform their job (e.g. need-to-know). Access to Restricted Information must be individually requested and then authorised in writing by the Information System Custodian. Restricted Information is highly sensitive and may have personal privacy considerations, or may be restricted by law. In addition, the negative impact on the institution should this Information be incorrect, improperly disclosed, or not available when needed, is very high.

University

The term 'University' or 'UniSQ' means the University of Southern Queensland.

University Members

Persons who include: Employees of the University whose conditions of employment are covered by the UniSQ Enterprise Agreement whether full time or fractional, continuing, fixed-term or casual, including senior Employees whose conditions of employment are covered by a written agreement or contract with the University; members of the University Council and University Committees; visiting, honorary and adjunct appointees; volunteers who contribute

	to University activities or who act on behalf of the University; and individuals who are granted access to University facilities or who are engaged in providing services to the University, such as contractors or consultants, where applicable.
	Definitions that relate to this procedure only
	Institutional Data All data owned or licenced by the University. **Security Classified Information Asset Register** A register, electronic or paper database that provides a record to log actions on Information Assets. **System** A combination of Information Assets and ICT Assets supporting a business process. **Users** Users are defined as all University Members, any person enrolled in an award course of study at the University and any person registered to attend short courses, seminars or workshops in any unit of the University as well as all other persons including members or the general public, who have been granted access to, and use of, the University's ICT Resources. A member of the public reading public University web pages from outside the University is not by virtue of that activity alone considered to be a User.
Keywords	
Record No	13/931PL