Information Asset and Security Classification Schedule

1 Purpose

To provide a high-level overview of default Sensitivity Classifications, additionally Information Systems responsibilities, indicative starting points for the assessment of the potential impact and a list of standard safeguards applicable to all data classification levels.

2 Scope

This Schedule must be read in conjunction with the Information Asset and Security Classification Procedure and is subordinate to it.

3 Schedule

3.1 Table 1: Information Assets, Custodians and Classifications

To assist with the process of managing new Information Assets, Table 1provides a high-level of the Core and Enabling Topics within the UniSQ Data Reference Model. For Foundational Topics, refer to the UniSQ Data Reference Model, accessible to all staff via the UniSQ Enterprise Information Management SharePoint site.

For new Information Assets not yet classified, Information Systems Custodians and/or Data Custodians (collectively referred to as an ISO) must firstly determine which Topic the new asset should be assigned to, then in consultation with the Information Asset Custodian, determine the appropriate Sensitivity Classification for the new asset.

Table 1. Default Classifications

Data Reference Model Topic	Information Asset Custodian	Default Sensitivity Classification
Curriculum	Deputy Vice-Chancellor (Academic Affairs)	Public
Student Attraction	Pro Vice-Chancellor (Engagement)	Official
Student Management	Associate Provost	Official
Learning and Teaching	Deputy Vice-Chancellor (Academic Affairs)	Official
Student Engagement and	Associate Provost	Official

Experience		
Planning and Performance	Director (Planning and Office of the Deputy Vice-Chancellor Enterprise Services), Enterprise Services Division	Official
Governance and Risk	Deputy Vice-Chancellor (Enterprise Services)	Official
Facilities	Executive Director (Facilities Management), Enterprise Services Division	Official
Services and Operations	Deputy Vice-Chancellor (Enterprise Services)	Public
Financial	Chief Financial Officer, Enterprise Services Division	Confidential
Legal and Compliance	Deputy Vice-Chancellor (Enterprise Services)	Confidential
Health, Medical and Counselling data	Associate Provost	Restricted Information
Assets	Deputy Vice-Chancellor (Enterprise Services)	Official
Advancement	Deputy Vice-Chancellor (Enterprise Services)	Public
Human Resources	Chief People Officer, Enterprise Services Division	Confidential
External Referencing	Vice-Chancellor Executive	Public

3.2 Table 2: Information Systems responsibilities

Once a new Information Asset has been classified, Information Systems Custodians and/or Data Custodians (ISO) must familiarize themselves with the responsibilities outlined in Table 2 with reference to section 4 of the Procedure.

Procedural References	Description	Information System Custodian or Data Custodian	ICT Services
4.1	Information Asset and Security classification	Determine classification with ICT Services	Classify as the owner with the ISO

4.2(1)	Unique Identification of Custodian	Assign most senior officer responsible for management	Confirm with ISO for major Systems/Applications
4.2(2)	Effective practices and training	Identify effective uses and provide regular training to users of Information System and Assets	Support training and University Communications of practices
4.2(3)	Monitor and Authorise Access	Manage user access with provided tools. Notify ICT Services of issues	Monitor and address audit issues. Action requests from ISO
4.2(4)	Compliance Obligations	Provide guidance on compliance	Assist in monitoring compliance and audits
4.2(5)	Information lifecycle management	Provide information export and integration assistance	Support information lifecycle infrastructure
4.2(6)	Central Authentication System	Report unprotected access	Implement authentication System
4.2(7)	Policy Instrument awareness	Advise Users of responsibilities and apply Principle of Least Privilege to Confidential and Restricted Information	Advise Users of relevant Policy Instruments and monitor access
4.2(8)	First Nations Data management	Identify and raise awareness about First Nations data and sovereignty	Support First Nations data management in accordance with regulatory, and national practices and guidelines

3.3 Table 3: Potential impact on the University

In order to preserve the confidentiality, integrity, and availability of Information Assets, and the University's reputation, Table 3 outlines security considerations should information be disclosed without authorisation.

Security Objective	LOW - Public	MODERATE - Official	MAJOR - Confidential	HIGH - Restricted
Confidentiality	**Limited or no** adverse effects.	**Serious** effects due to exposure	**Major effect** due to exposure of	**Severe effect** due to exposure

		of administrative data about University, students or staff.	personally identifiable information or information of strategic significance to the University.	of sensitive information with regulatory cyber security ramifications.
Integrity	**Modification or destruction of Information** could be expected to have a **limited or no** adverse effect.	**Modification or destruction** of Information could be expected to have a **serious** adverse effect due to impact on administrative data.	**Modification or destruction** of Information could be expected to have a **major** effect due to impact to personally identifiable information or information of strategic significance to the University.	**Modification or destruction** of Information could be expected to have a **severe** effect due to impacts on of sensitive information with regulatory cyber security ramifications.
Availability	**Limited or no impacts** with disruptions of access; causes mild inconvenience to users.	**Disruptions of access** have **serious** adverse effect as official operations are delayed.	**Disruptions of access** have **major** effects; causes inability to access information of strategic importance.	**Disruptions of access** have **severe** effects; causes inability to access critical information.
Reputation	No media coverage. Customer complaints within normal levels.	Limited national media coverage and/or customer loss. Large increase in customer complaints.	National or international media coverage and/or large scale customer loss leading to material decline in revenue. VCE involvement in remediation.	Sustained national and international media coverage and/or large scale customer loss leading to material decline in revenue. Council involvement in remediation.

3.4 Table 4: Safeguards for protecting data and data collections based

on their classification

The below represents a standard set of safeguards applicable to data classifications levels. These must be considered by the ISO and an appropriate control set applied to meet control objectives, business requirements and risk assessment.

Controls	Public	Official	Confidential	Restricted
Network Security	Data may reside on public networks; minimal security required.	A firewall is required to protect data, with monitoring for unauthorised access.	A network firewall is essential, and additional protective measures, such as intrusion detection/prevention systems (IDS/IPS), must be implemented.	Strict firewall rules are mandated; servers hosting data must not be visible to public networks or unprotected subnets.
System Security	Basic best practices for system management are recommended to maintain data integrity.	University-specific best practices are required to secure systems and protect sensitive data.	Compliance with established University best practices is mandatory to ensure data confidentiality and integrity.	All systems must adhere to the highest standards of security management to safeguard restricted data.
Remote Access	No restrictions on remote access; data can be accessed from any location.	Remote access is restricted to local networks or through Virtual Private Networks (VPNs) to ensure secure connections.	Limited access for third parties is allowed only under specific, authorised conditions.	Remote access is strictly controlled and monitored; unauthorised access is not permitted.
Copying/Printing	No restrictions; data can be copied or printed without formal procedures.	Data should only be printed when there is a legitimate need; copies must be limited to UniSQ staff and not left unattended.	Data only to be printed when there is a legitimate need; copies must be limited to individuals with delegated access rights relevant to their roles, and should be labelled "CONFIDENTIAL."	Data should only be printed when necessary; copies are limited to individuals authorised to access the data and must be labelled "RESTRICTED."

Data Storage	Data is recommended to be stored on secure servers to minimise risks.	Storage in secure Data Centres is mandatory to protect sensitive information.	Data must be stored in secure Data Centres, with strict access controls to ensure protection against unauthorised access.	Data must be kept in highly secure Data Centres, with compliance to the strictest security protocols.
Transmission	No restrictions apply to data transmission.	No specific requirements are necessary for transmission; however, encryption is recommended for sensitive communications.	Encryption is required for transmitting data (via SSL or secure file transfer protocols), and cannot be transmitted via email unless encrypted and secured with a digital signature.	Encryption is required for all transmissions; similar restrictions apply regarding email transmission.
Backup/Disaster recovery	Backups not required; data can be stored without formal procedures.	Daily incremental backups are recommended; weekly full backups are recorded and monitored.	Daily backups are required, with backup media stored securely across multiple locations to ensure recovery capabilities.	Daily backups are mandatory, with strict protocols in place for secure storage and recovery.
Retention	No restrictions; data can be retained indefinitely.	Data must be retained in accordance with official business requirements for the Information Asset.	Retention must comply with legislative requirements pertinent to the Information Asset; all assets should adhere to the Queensland General Retention and Disposal Schedule.	Destruction of electronic media must follow strict protocols, with documentation required for compliance.
Disposal	No restrictions; data can be disposed of without formal procedures.	Reports containing sensitive information must be shredded; electronic media must be securely erased.	Destruction of electronic media must be conducted in compliance with security protocols to ensure data is irrecoverable.	All data disposals must follow rigorous protocols to prevent unauthorised access to sensitive information post-

				disposal.
Register/Audit Logs	Audit logs are not required for public information.	Basic logging of access is required to ensure accountability	Detailed logging must include the information asset owner, security classification, and reasons for classification.	Comprehensive audit logs are mandatory, including detailed activity logs for access, modifications, and disposals, to ensure accountability and traceability.

Audit Log Controls

Control Type	Administrator	General Use
Log Access	Logs login/logout and file access; administrators must not have Read, Write, Modify, or Delete access to audit logs.	Logs login/logout and failed attempts; users may have restricted access based on their role.
File Access	Logs all administrative access actions; further controls are implemented to ensure log integrity.	Logs file access and modifications, including failed attempts. Users may have varying levels of access based on their roles.

4 References

Queensland Government. *General Retention and Disposal Schedule (GRDS)*. Retrieved June 2024 from https://www.forgov.qld.gov.au/information-and-communication-technology/recordkeeping-and-information-management/recordkeeping/disposal-of-records/search-for-a-retention-and-disposal-schedule/general-retention-and-disposal-schedule-grds

Queensland Government. *University Sector Retention and Disposal Schedule*. Retrieved June 2024 from https://www.forgov.qld.gov.au/information-and-communication-technology/recordkeeping-and-information-management/recordkeeping/disposal-of-records/search-for-a-retention-and-disposal-schedule/university-sector-retention-and-disposal-schedule

5 Schedule Information

Accountable Officer	Chief Information Officer

Responsible Officer	Chief Information Officer
Policy Type	University Procedure
Policy Suite	ICT Information Management and Security Policy
Approved Date	24/1/2025
Effective Date	24/1/2025
Review Date	24/1/2030
Relevant Legislation	
Policy Exceptions	Policy Exceptions Register
Related Policies	Records and Information Management Policy
Related Procedures	Research Data and Primary Materials Management 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 Privacy website
Definitions	**Terms defined in the Definitions Dictionary**
	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 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 schedule only

	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	15/3204PL

Failure to comply with this Policy or Policy Instrument may be considered as misconduct and the provisions of the relevant Policy or Procedure applied. A hard copy of this electronic document is uncontrolled and may not be current as UniSQ the University regularly reviews and updates its Policies and Policy Instruments. The latest controlled version can be found in the UniSQ's Policy and Procedure Library.