Information Asset and Security Classification Schedule

University of Southern Queensland

1 Purpose

To provide a high-level default classification for each of the functional areas (Table 1), details regarding Information Systems responsibilities (Table 2), indicative starting points for the assessment of the potential impact (Table 3) and a list of standard safeguards applicable to all data classification levels (Table 4).

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: Functional area responsibility and Information System Custodian

Table 1 provides a high-level default classification for each of the functional areas mentioned. These should be used as indicative starting points for the assessment of the potential impact (Table 3) for the further detailed classification for individual Systems within the functional areas.

Functional Area	Information System Custodian	Classification
Academic data	Provost and Head of College and Dean (Pathways Education)	Restricted Information
Alumni data	Pro Vice-Chancellor (Engagement)	Restricted Information
Corporate Website and Content Management	Pro Vice-Chancellor (Engagement)	Public Information
Course Material, Learning Management data	Provost and Head of College and Dean (Pathways Education)	Internal Information
Facilities and Services data	Executive Director (Facilities Management), Enterprise Services Division	Restricted Information
Financial data	Chief Financial Officer, Enterprise Services Division	Restricted Information

Health, Medical and Counselling data	Dean (Students)	Restricted Information
People Portfolio data	Chief People Officer, Enterprise Services Division	Restricted Information
Information Technology data	Chief Information Officer, Enterprise Services Division	Restricted Information
Library data	Director (Library Services), Academic Division	Public Information
Planning data	Director (Planning and Office of the Deputy Vice-Chancellor Enterprise Services), Enterprise Services Division	Restricted Information
Process data	Director (Planning and Office of the Deputy Vice-Chancellor Enterprise Services), Enterprise Services Division	Internal Information
Registered Records (Enterprise Information Management Services)	Chief Information Officer, Enterprise Services Division	Restricted Information
Research data and Research information	Deputy Vice-Chancellor (Research and Innovation)	Restricted Information
Student data	Deputy Academic Registrar and Director (Student Administration)	Restricted Information

3.2 Table 2: Information Systems responsibilities

Internal Procedural References	Description	Information System Custodian	ICT Services
4.1	Information System classification	Determine a classification in conjunction with ICT Services	Where ICT Services is the owner, classify the System appropriately. Where not, classify the System in conjunction with the ISO
4.2(1)	Unique identification and designation of Information System Custodian for each Information System/applicatio	Within the relevant functional area, the most senior officer or Employee responsible for the management of a faculty or a management or support service or administrative area or sub-section of which that is specifically identified for	In conjunction with the business and appropriate stakeholders, confirm ISO for all major Information Systems/Applications

	n	allocation of funding within the University's budget framework is assigned the role of the ISO	
4.2(2)	Monitoring the University's ICT network infrastructure and addressing audit issues	No responsibility, except to notify ICT Services if they become aware of any network infrastructure issues or concerns	Monitor the University's ICT network infrastructure and address audit issues related to this
4.2(3)	Monitoring, authorising and revoking access and addressing audit issues	Monitor, authorise and revoke user access as required with the tools and means provided by ICT Services	Actioning requests from the ISO, and providing ISO with the means to either perform the tasks or perform the tasks requested by the ISO
4.2(4)	Avoid breaches of legal, statutory, regulatory, contract or privacy obligations	Work in conjunction with ICT Services, to provide guidance as to compliance with respect to legal, statutory, regulatory, contract or privacy compliance obligations	Assist ISO in monitoring compliance to obligations with regard to University's Information Systems and Information Assets, and assist in internal and/or external audits, including reporting on the status of audit issues
4.2(5)	Central Authentication System	No responsibility to implement System, but bring to the attention of ICT Services if it is found that a restricted System can be accessed without authenticating	Ensure that the centralised authentication System is implemented and that restricted Systems are only accessible after Users have authenticated through the System
4.2(6)	Policy/procedure awareness	Advise University Users of security responsibilities specific to the System	Advise University Users of the relevant ICT security policy/procedures and general security responsibilities
4.2(7)	Employee training	Ensure that Employees using the System are trained in its use	Ensure that Employees using ICT Systems are trained

3.3 Table 3: Potential impact on the University

Security Objective	LOW - Public	MODERATE - Internal	HIGH - Restricted
Confidentiality Preserving authorised restrictions on Information access and disclosure, including means for protecting personal privacy and proprietary Information	The unauthorised disclosure of Information could be expected to have **limited or no** adverse effect on the University operations, assets or individuals	The unauthorised disclosure of Information could be expected to have a **serious** adverse effect on University operations, assets or individuals	The unauthorised disclosure of Information could be expected to have a **major or severe effect** on University operations, assets or individuals
Integrity Guarding against improper Information modification or destruction, and includes ensuring Information non-repudiation and authenticity	The unauthorised **modification or destruction of Information** could be expected to have a **limited or no** adverse effect on University operations, assets or individuals	The unauthorised **modification or destruction** of Information could be expected to have a **serious** adverse effect on University operations, assets or individuals	The unauthorised **modification or destruction** of Information could be expected to have a **major or severe** effect on University operations, assets or individuals
Availability Ensuring timely and reliable access to and use of Information	The **disruptions of access** to or use of Information/System could be expected to have a **limited or no** adverse effect on University operations, assets or individuals	The **disruptions of access** to or use of Information/System could be expected to have a **serious** adverse effect on University operations, assets or individuals	The disruptions of access to or use of Information/System could be expected to have a **major or severe** effect on University operations, assets or individuals
Reputation	No media coverage. Customer complaints within normal levels.	Limited national media coverage and/or customer loss. Large increase in customer complaints.	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.

	Public Information	Internal Information	Restricted Information
Access Controls	No restriction for viewing Authorisation by ISO required for modification	Viewing and modification restricted to authorised individuals as needed for business related roles ISO grants permission for access Appropriate authentication and authorisation required for access	Viewing and modification restricted to authorised individuals as needed for business related roles on a need-to-know basis ISO grants permission for access with appropriate authentication and authorisation UniSQ Confidentiality Agreement required to be signed by contractors and lodged with the Legal Office
Network Security	May reside on a public network Protection with a firewall IDS/IPS protection is recommended	Protection with a network firewall required IDS/IPS protection required Servers hosting the data should not be visible to entire Internet May be in a shared network server subnet with a common firewall rule set for the set of servers	Protection with a network firewall using 'default deny' rule set required IDS/IPS protection required Servers hosting the data cannot be visible to the entire Internet, nor to unprotected subnets like the residence halls and guest wireless networks Must have a firewall rule set dedicated to the System The firewall rule set should be reviewed periodically
System Security	Must follow general best practice for System management	Must follow University-specific best practice for System management and security Host-based software firewall	Must follow University-specific best practice for System management and security Host-based software firewall

	and security Host-based software firewall recommended Current antivirus	required Host-based software IDS/IPS recommended Current antivirus	required Host-based software IDS/IPS recommended Current antivirus File integrity checker
Remote Access	No restriction for Public facing Systems	Access restricted to local network or VPN Remote access by 3rd party for technical supported limited to authenticated VPN secure protocols, e.g. SSL	Additional, Unsupervised remote access by 3rd party for technical support not allowed
Copying/Printing	No restriction	Data should only be printed when there is a legitimate need Copies must be limited to individuals with a need-to-know Data should not be left unattended on a printer/fax May be sent by Internal mail	Data should only be printed when there is a legitimate need Copies must be limited to individuals authorised to access the data and have a signed UniSQ Confidentiality Agreement Data should not be left unattended on a printer/fax Copies must be labelled 'CONFIDENTIAL' May be sent via a Confidential envelope
Data Storage	Storage on a secure server recommended	Additional, Storage in a secure Data Centre recommended NOT stored on an individual's PC or mobile device	Additional, Storage on a secure server in a secure Data Centre required Not on a PC or personal device unless using whole-disc encryption Encryption on back-up media required if taken off-site
Transmission	No restriction	No requirements	Encryption required (via SSL

			or secure file transfer protocols) Cannot transmit via email unless encrypted and secured with a digital signature
Backup/Disaster recovery	Backups required Daily incremental recommended. Weekly full recorded	Daily backups required Backup tapes are stored across 3 buildings on the Toowoomba Campus. The tape library and tape drives reside in a dedicated back-up room on a purpose-built site within the Toowoomba campus	Daily backups required Backup tapes are stored across 3 buildings on the Toowoomba Campus. The tape library and tape drives reside in a dedicated back-up room on a purpose-built site within the Toowoomba campus
Disposal	No restrictions	Shred reports Wipe/erase or destroy electronic media; hard drives, USBs, CD and DVDs, printer drums, magnetic media	Shred reports Destruction of electronic media
		Note: All disposals of data (electronic and hard copy) must be made in accordance with the approved Disposal Schedule and recorded on the Records Disposal Register Form	
Register/Audit Logs	Not required	As a minimum, the Register should include: • Information Asset Owner • name or unique identifier of asset or group of assets • description of Information Asset • location of Information Asset • security classification of the Information Asset	Additional Information is required for Restricted category assets: Audit Logs containing • Full details of logged Information on activity for Access, Modify, Delete • number of copies in circulation and their location • disposal details where Information Asset has been disposed of

		• date of security classification with details of the authority of the classifier • reason for the security classification of the Information Asset, including legislative, regulatory, policy or other reference where applicable, or a copy of the impact assessment made • date to review security classification	For Restricted Information Assets, the ISO owner must either conduct a spot check of a small sample of Restricted Information Assets to ensure that these are accounted for and are being handled, stored, in accordance with the minimum standards set out in this framework
Audit Log Controls (Administrator)	Log in/out, File Access, Administrators are not to have Read, Write, Modify or Delete access to audit logs		
Audit Log Controls (General User)	Log in/out, Failed attempts	Log in/out, Failed attempts, Delete	Log in/out, Failed attempts, Read, Write, Modify and Delete

4 References

Nil.

5 Schedule Information

Accountable Officer	Chief Information Officer
Responsible Officer	Chief Information Officer
Policy Type	University Procedure
Policy Suite	Enterprise Architecture Policy
Approved Date	31/1/2022
Effective Date	31/1/2022
Review Date	17/10/2028

Relevant Legislation	
Policy Exceptions	Policy Exceptions Register
Related Policies	ICT Information Management and Security Policy Records and Information Management Policy
Related Procedures	Research Data and Primary Materials Management Procedure
Related forms, publications and websites	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

Is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

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