Information Asset and Security Classification Procedure

1 Purpose

To establish a process for classifying and handling University Information Assets based on its level of sensitivity, value and criticality to the University.

These procedures outline the specific actions and processes that will assist Information Systems Owners implement the ICT Information Management and Security Policy requirements in relation to Information Asset management and Information Classification.

2 Scope

This procedure applies to all Users who access, process, or store sensitive University Information.

3 Procedure Overview

This procedure outlines the Information Asset and Security classification process to be adopted by the University and the processes involved in implementing this process.

4 Procedures

4.1 Information Asset and Security Classification framework

The goal of Information Security is to protect the confidentiality, integrity and availability of Information Assets and Information Systems. Information Asset classification reflects the level of impact to the University if confidentiality, integrity or availability is compromised.

Information Asset classification, in the context of Information Security, is the classification of Information based on its level of sensitivity and the impact to the University should that Information be disclosed, altered, or destroyed without authorisation. The classification of Information helps determine what baseline Security Controls are appropriate for safeguarding that Information. All Institutional Information should be classified into one of three sensitivity tiers, or classifications.

- Tier 1: Public Information
- Tier 2: Internal Information

- Tier 3: Restricted Information

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

The University is required to comply with Information Privacy Principles under Queensland legislation. As a result the default classification for the treatment of Personal Information will be deemed Restricted Information pending completion of a privacy threshold assessment.

4.2 Accountabilities and responsibilities

All University Employees must be conscious of the Information Classification that has been allocated to a specific Information System and must ensure that they do not breach the controls that have been implemented for that system.

1. All Information Systems and Information Assets must be uniquely identified, assigned an Information System Custodian and given an Information Classification. Information Asset and Security Classification Schedule -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 (Information Asset and Security Classification Schedule - Table 3) for the further detailed classification for individual systems and/or assets within the functional areas. The Information System Custodian is responsible for the adherence to the ICT Information Management and Security Policy.

2. ICT Services is responsible for monitoring the University's ICT network infrastructure, including all hardware and communications links, and addressing any audit issues that may be identified in relation to these items.

3. Information System Custodians are responsible for ensuring that appropriate controls are in place for monitoring their Information System and/or Information Assets, authorising and revoking access (for Information Systems classified as Restricted Information) and addressing any audit issues that may be identified, with the assistance of ICT Services.

4. To avoid breaches of legal, statutory, regulatory, contract or privacy obligations the Executive Director, ICT Services will ensure that:
    a. ICT Services will monitor compliance to obligations with regard to the University's ICT network infrastructure.

    b. ICT Services will assist Information System Custodians in monitoring compliance to obligations with regard to University's Information Systems and Information Assets as required.

    c. Assistance is provided as required for the purpose of internal and/or external

audits, including reporting on the status of audit issues.

5. The Executive Director, ICT Services is responsible for ensuring that a central authentication System (such as usernames and passwords for the network) is available and provides secure access by University clients to Information Systems classified as Internal Information.

6. All University Users who are to have access to the University's Information Systems are to be made aware of the ICT Information Management and Security Policy and this procedure and their responsibility for maintaining Information Security.

7. Each Information System Custodian is to ensure that staff are trained in the effective use of their Information System.

4.3 Security classification process

4.3.1 Identify Information System Custodians

Responsibility for ensuring that Information Assets have a security classification is authorised by the Information System Custodian (refer to Information Asset and Security Classification Schedule - Table 1). Information Assets should be classified by the Information System Custodian at the earliest possible opportunity according to the sensitivity of the Information Asset.

In the case of Information Assets externally generated, and not otherwise classified, the University officer who receives the Information Asset should approach the Information System Custodian to classify the Information Asset and guide its control within the University.

4.3.2 Identify Information Assets

Identify the Information Asset in accordance with Information Asset and Security Classification Schedule - Table 2.

4.3.3 Assess data vulnerabilities/risks

Perform a risk assessment and consider the vulnerabilities that are attributed to each Information Asset (refer to Information Asset and Security Classification Schedule - Table 3).

Relevant data security issues for the Information System Custodian to consider might include:

- data control
- data encryption
- blending of data with other customer data

- business process if a security breach does occur or if data is damaged or destroyed
- data backup frequency/conventions/standards/accessibility
- availability of an audit trail to demonstrate that University data is reliable.

4.3.4 Apply data classification to Information Asset

The highest security classification level determined by the impact assessment must be applied to that Information Asset. Unlike a risk assessment, data security classification is determined by the perceived level of impact to the organisation or individual (refer to Information Asset and Security Classification Schedule - Table 3).

4.3.5 Apply controls

Listed below are details of controls which should be applied to ensure that appropriate protection is given to the Information Asset.

- The **need-to-know** principle requires that Information Assets should only be available to those who need to use or access the Information Asset to do their work.
- A **clear desk policy** requires that classified Information Assets are secured and that unauthorised Users are not able to access any electronic material, System or network to which the User had been connected.
- Where the University is required to handle security classified Information Assets from external organisations, the Information Assets must be treated in the following ways:
    - Retain the security classification as forwarded.
    - Manage the Information Assets according to the USQ Confidentiality Agreement, between the organisations. The originator of the data transfer is responsible for ensuring that its Information Assets will be properly protected.
    - For each classification, several data handling requirements are defined to appropriately safeguard the Information. Information Asset and Security Classification Schedule - Table 4 defines the required safeguards for protecting data and information collections based on their classification.

4.3.6 Audit logs

To maintain confidentiality and integrity of classified Information Assets a strict audit logging process is to form part of the Security Classified Information Asset Register. This audit log must be carefully designed to ensure it is capable of providing a 'trail of evidence' which can be used

to investigate inappropriate or illegal access.

Audit log access controls must be in place with explicit user authentication needed to view the audit log database (Information Asset and Security Classification Schedule - Table 4).

4.3.7 Disposal of Information Assets

To ensure security and confidentiality, the disposal of Information Assets in any form must follow the guidelines outlined in Information Asset and Security Classification Schedule - Table 4.

4.4 Education and awareness

To ensure that University Users are informed of the importance of security classifying Information Assets, an ongoing education and awareness program will be undertaken by ICT Services.

4.5 Information Asset Register

The University is committed to making information accessible to the community to support openness, accountability and transparency. The University provides details regarding information collected in the course of managing a public university and meeting the University's mission of enabling broad participation in higher education and to make significant contributions to research and community development.

Access to the Information within the listed Information Assets contained in the Information Asset Register is aligned with Queensland legislative requirements.

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 is available on the Right to Information and Privacy websites.

4.5.1 Maintaining the Information Asset Register

Responsibility for ensuring that Information Assets listed in the Information Asset Register are reviewed, updated and maintained annually remains the responsibility of the Information System Custodian (refer to Information Asset and Security Classification Schedule - Table 1).

5 References

Nil.

6 Schedules

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

7 Procedure Information

Accountable Officer	Executive Director (ICT Services)
Responsible Officer	Executive Director (ICT Services)
Policy Type	University Procedure
Policy Suite	Enterprise Architecture Policy
Subordinate Schedules	Information Asset and Security Classification Schedule
Approved Date	20/10/2017
Effective Date	20/10/2017
Review Date	30/10/2018
Relevant Legislation	AS ISO/IEC 27000:2014 - Security technology-Security techniques-Information security management systems-Overview and vocabulary AS ISO/IEC 27001: 2015 - Security techniques-Information security management systems-Requirements AS ISO/IEC 27002: 2015 - Information technology-Security techniques-Code of practice for information security controls AS ISO/IEC 27005: 2011 - Information technology-Security techniques-Information security risk management *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 2002* *Public Sector Ethics Act 1994*

	Queensland Government Information Security Classification Framework Queensland Information Standard 02: 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 26: Internet Queensland Information Standard 31: Retention and Disposal of Public Records 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 2009* *University of Southern Queensland Act 1998*
Related Policies	Acceptable use of ICT Resources Policy Code of Conduct Policy Delegations Policy Fraud and Corruption Management Policy ICT Information Management and Security Policy Privacy Policy Public Interest Disclosure Policy Records and Information Management Policy Right to Information Policy

	Risk Management Policy and Procedure Student Communication Policy
Related Procedures	Disciplinary Action for Misconduct or Serious Misconduct Procedure Research Data and Primary Materials Management Procedure Student Communication Procedure Use of Electronic Mail Procedure
Related forms, publications and websites	Australian Government National e-Authentication Framework (under development by Digital Transformation Office) Disposal Schedules Enterprise Information Management Framework (EIM Framework) Information Asset Register Records Disposal Register Form Right to Information website Privacy website USQ Confidentiality Agreement (restricted access)
Definitions	**Terms defined in the Definitions Dictionary**
	Employee A person employed by the University and whose conditions of employment are covered by the USQ 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

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 'USQ' means the University of Southern Queensland.

	University Members Employees of the University whose conditions of employment are covered by the USQ 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 and adjunct academics; Volunteers who contribute to University activities or who act on behalf of the University; Individuals who are granted access to University facilities or who are engaged in providing services to the University, such as contractors and 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