ICT Services
Electronic Data Management Guideline

Trim Location:	<Insert TRIM Location>
Document Category*:	Guideline
Purpose*:	These guidelines outline the specific actions and processes that must be followed to implement the USQ Policy for ICT Information Management and Security Electronic Data Asset Management. This guideline will be reviewed on an annual basis and evaluated in line with changes to business processes and planning requirements.
Responsible Officer*:	Executive Director, ICT Services

1 Guideline Statement

This guideline provides additional details on the *USQ Policy for ICT Information Management and Security* in relation to the policy, planning and governance and information asset management. Specifically this guideline enables the implementation of an appropriate level of security classification of information asset management dealing specifically with electronic data assets ensuring a consistent approach in dealing with the sensitivity and confidentiality of all USQ electronic data.

2 Principles

2.1 Information System Classification

Each Information System will require its own level of security based on its Information Classification. The University classifies Information Systems within the following categories:

a) Public – information of a nature which does not warrant any restrictions on access from the community at large (e.g. the corporate website).
b) Internal (University Clients) – information which relates to University activities and which is of relevance in terms of application to or use by all members of the University community.
c) Restricted – information generated or utilised in the operation of University functions or business activities which require restrictions based on functional need, institutional risks and legislative requirements (e.g. personal privacy, commercial value, etc). Access may be necessary by a range of University Stakeholders to carry out University activities. Examples may include staff and student personal information, financial information, information on commercial dealings or activities, and audit information.

   Note: All third-party access requests to restricted information must be referred to the Manager, Corporate Records for appropriate action.

2.2 Accountabilities and Responsibilities

a) All Information Systems must be uniquely identified, assigned an Information System Owner and given an Information Classification. The Information System Owner is responsible for the adherence to the *USQ Policy for ICT Information Management and Security* in relation to the Information System for which they are assigned. The University's Information Systems, their responsible Information System Owners and their Information Classification will be identified in the Schedule: Functional Area, Information System Owners and Classification, and indicative (but not exhaustive) responsibilities of ICT Services and the Information System Owner for each part of this guideline are identified in Schedule: Functional Area, Information Systems Responsibilities.
b) 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.
c) Information System Owners are responsible for monitoring their Information System, authorising and revoking access (for Information Systems classified as Restricted) and addressing any audit issues that may be identified, with the assistance of ICT Services.

d) To avoid breaches of legal, statutory, regulatory, contract or privacy obligations the Executive Director, ICT Services will ensure that:
   - ICT Services will monitor compliance to obligations with regard to the University's ICT network infrastructure;
   - ICT Services will assist Information System Owners in monitoring compliance to obligations with regard to University's Information Systems and Information Assets as required; and
   - Assistance is provided as required for the purpose of internal and/or external audits, including reporting on the status of audit issues.

e) 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.

f) All University Clients who are to have access to the University's Information Systems are to be made aware of the *USQ Policy for Information Management and Security* and this guideline and their responsibility for maintaining information security.

g) Each Information System Owner is to ensure that staff are trained in the effective use of their Information System.

Schedule: Functional Area, Information System Owner and Classification

Functional Area	Information System Owner	Classification
Academic data	Senior Deputy Vice Chancellor Academic Programs	Restricted
Alumni data	Deputy Vice Chancellor Research and Innovation (Director External Relations)	Restricted
Corporate Website and Content Management	Director Marketing & Student Attraction, Students and Communities Division	Public
Course Material, Learning Management data	Deputy Vice Chancellor Academic Services (Pro Vice-Chancellor (Learning Teaching & Quality)	Internal
Facilities and Services data	Executive Director- Campus Services, University Services Division	Restricted
Financial data	Chief Financial Officer, University Services Division	Restricted
Human Resources data	Executive Director- Human Resources, University Services Division	Restricted
Information Technology data	Executive Director- ICT Services, Academic Services Division	Restricted
Library data	Executive Director – Library Services, Academic Services Division	Public
Planning data	Group Manager - Sustainable Business Management & Improvement, University Service Division	Restricted
Registered Records (Corporate Records)	Group Manager - Sustainable Business Management & Improvement, University Service Division (Manager Corporate Records)	Restricted
Research data	Deputy Vice Chancellor Research and Innovation (Director Office of Research and Higher Degrees)	Restricted
Student data	Deputy Vice Chancellor Students and Communities	Restricted

Schedule: Information Systems Responsibilities

Guideline Reference	Description	Responsibilities – Information System Owner (ISO)	Responsibilities – ICT Services
2.1	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.
2.2a	Unique identification and designation of Information System Owner for each information system/application.	Within the relevant functional area, the most senior officer or member of staff 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 allocation of funding within the University's budget framework is assigned the role of the Information Systems Owner.	In conjunction with the business and appropriate stakeholders, confirm ISO for all major Information Systems/Applications.
2.2b	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.
2.2c	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.
2.2d	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.
2.2e	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.
2.2f	Policy awareness.	Advise University Clients of security responsibilities specific to the system.	Advise University Clients of the security policy and general security responsibilities.
2.2g	Staff training.	Ensure that staff using the system are trained in its use.	Ensure that staff using ICT systems are trained

3 Definitions

Word/Term	Definition (with examples if required)
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 on ICT Assets and recognised as having value for the purpose of enabling USQ to perform its business functions, thereby satisfying a recognised USQ requirement.
Information Classification	The categorisation of an Information Asset for the purposes of identifying 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 Owner	The nominated individual that has responsibility for the security of the data and application component of the Information Asset and is also accountable for those aspects of Information Security.
Information Systems	The organised collections of hardware, software, equipment, policies, procedures and people that store, process, control and provide access to information.
Public record (refer Section 6, Public Records Act 2002)	A public record is any form of recorded information that provides evidence of the decisions or actions of a 'public authority' (in this case USQ) in undertaking its business activities or in the conduct of its affairs. The Act includes all records (and information) irrespective of the form, the custodial arrangements and the technology used to generate, manage, preserve and access records.
Security Classified Information	Information which has been assessed against the Queensland Government Information Security Classification Framework (QGISCF) and assigned a classification
Secure Area	Provides the highest integrity of access to, and audit of, Security Classified Information Assets to ensure restricted distribution and to assist in subsequent investigation if there is unauthorised disclosure or loss of information assets. The essential physical security features of a Secure Area include: • appropriately secured points of entry and other openings • tamper-evident barriers, highly resistant to covert entry • an effective means of providing access control during both operational and non-operational hours • all persons to wear passes • all visitors escorted at all times • during non-operational hours a monitored security alarm system, providing coverage for all areas where Security Classified information assets are stored • an approved means of limiting entry to authorised persons.
Stakeholders	all staff, students, contractors, third parties, clinical and adjunct title holders, affiliates, alumni and all other individuals who access USQ's systems and/or network.
System	A combination of Information Assets and ICT Assets supporting a business process.