

(Standard) ICT Standard for Information Asset Classification and Control

Document Purpose

Document Purpose	To define guidelines for the classification and management of sensitive information that is handled created, received and/or destroyed by the University of Southern Queensland (USQ) in accordance with its sensitivity, confidentiality of content and business importance. Based upon legislative, regulatory and contractual requirements.			
Document Information	Version	1.0		
	Release Date	November 2009		
	Release Status	Final		
	Review Date	November 2010		
	Author(s)	Principal Manager – Infrastructure and Systems		
	Owner	Principal Manager – Infrastructure and Systems		
	Print Date	Last Printed: 21/06/2010 12:24:00 PM		
	Approved By	Principal Manager – Infrastructure and Systems		
	Policy	USQ Policy for ICT Information Management and Security		
	Type of Document	Standard		
	Electronic Location and Filename	http://www.usq.edu.au/resources/ict_standard_for_information_asset_classification_and_control.pdf		
Version Control	Version	Date	Author(s)	Summary of Changes
	0.1	2008	Various	Document creation
	1.0	July 2008	Maggie Fryer	Final Release
Error Advisory	<p>To the Reader:</p> <p>If you encounter any inaccuracies or printing faults in this document please contact the Owner (see Document Information section, above) as soon as possible. The Owner will then initiate the required modifications</p> <p>If you are unable to contact the Owner, contact that person's Manager Supervisor.</p> <p>Thank you for helping the Division of ICT Services maintain quality documentation.</p>			

Table of Contents

- Document Purpose 1**
- Document Information 1**
- Error Advisory 1**
- 1 Definitions..... 3**
- 2 Introduction 3**
- 3 Standards..... 4**
 - 3.1 Information Asset Security Classification Controls 7
 - 3.1.1 Public 7
 - 3.1.2 Unclassified 8
 - 3.1.3 Classified - Secure 10
 - 3.1.4 Classified - Sensitive 12
- 4 Related Documents..... 15**

1 Definitions

The *ICT Glossary and Definitions* contains a description of any common ICT terminology referred to in the policy and standard documentation.

2 Introduction

'Information Assurance' is concerned with the protection of information and information systems by ensuring availability, integrity, authentication, confidentiality and non-repudiation of information operations.

It includes providing for restoration of information systems by the incorporation of appropriate protection, detection and reaction capabilities.

Principle 3 (Information Asset Classification and Control) of the Queensland Government Information Standard IS18 (Information Security) requires agencies to implement policies and procedures for the classification and protective control of information assets (in electronic and paper-based formats) which are commensurate with their value, importance and sensitivity.

All physical information assets (including hardware and software) used to process, store or transmit information must be accounted for as per the *Financial Administration and Audit Act 1977 (FAA)*.

In addition to asset inventories required by the FAA, all major University information assets used in University operations must be identified and an owner assigned for the maintenance of appropriate security controls.

3 Standards

1. Inventories of all major information and ICT assets should be maintained.
2. Information will be classified according to its sensitivity and importance, taking into account University requirements for the sharing or restriction of information, legal and/or legislative requirements and probable impact resulting from unauthorised access or damage to the information.

To achieve and maintain appropriate protection of the University information organisational assets

- a. All assets shall be clearly identified and an inventory of all important assets drawn up and maintained;
 - b. The University will adopt the *Business Classification Scheme* for the purposes of classification of USQ 'public records' and disposal schedules;
 - c. All information and assets associated with information processing facilities shall be 'owned' by a designated part of the organisation. The owner shall be a Corporate Executive Portfolio Steward/ Principal Activity Steward/System Sponsor or ICT Manager;
 - d. Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented. See also the *ICT Standard for the Use of ICT Resources*.
3. The University will refer to the Queensland Government Information Security Classification Framework 'The Security Classification Schema' as the basis for our information classification scheme with the following qualifications:
 - a. Information will be classified as either Public or Non-Public;
 - b. Non-Public Information will be classified as either Unclassified or Classified;
 - c. Classified Information will be classified as either Secure (instead of Highly Protected or Protected) or Sensitive (instead of X-in-Confidence).
 4. Confidentiality, integrity and availability of sensitive or secure information will be appropriately protected throughout the information lifecycle: collection; storage; use; transmission; disposal.
 5. If information is stored in the Data Centre, the security classification will be commensurate with the zone where the information is located.
 6. The Corporate Executive Portfolio Steward/Principal Activity Steward/System Sponsor is responsible for ensuring an information technology resource and/or the information contained within, is classified as: Public; Sensitive; or Secure Information. Security measures will be implemented according to the information classification.
 7. Sensitive or secure information will be appropriately protected independent of location and technology.

To ensure that information receives an appropriate level of protection

- a. Information shall be classified in terms of its value, legal requirements, sensitivity and criticality to the University.
 - b. An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification system adopted by the University.
8. Authority to lower an information classification must be obtained from the Corporate Executive Portfolio Steward/Principal Activity Steward/System Sponsor of the information source
 9. Personal information defined by the Australian Privacy Act or Queensland Government Information Standard 42 - Information Privacy, shall be classified as at least sensitive information.

10. Core Information Systems will be identified and information assurance responsibility assigned to the Core System Sponsor unless otherwise indicated.
11. University Staff should agree to a confidentiality agreement prior to commencement of formal duties and the agreement should be reviewed annually or whenever there is a change in terms of employment
12. Classification schemes do not limit the provision of relevant legislative requirements under which the University operates.
13. Disposal of public records shall be in accordance with the [USQ Records Disposal Policy](#)
14. The archiving of information and documents shall be in accordance with the [USQ Archives Policy and Procedures](#).
15. Storage media used for the archiving of information must be appropriate to its expected longevity. The format in which the data is stored must also be carefully considered, especially where proprietary formats are involved.
16. Removal off site of the organisation's sensitive information assets, either printed or held on computer storage media, should be properly authorised by management. Prior to authorisation, a risk assessment based on the criticality of the information asset should be carried out. At a minimum, where information is classified as "Classified – Secure" or "Classified – Sensitive", a Confidentiality Agreement between the University and the Organisation contracted to perform services for the University where access to this information is required shall be signed and processed through the USQ Legal Office.
17. Responsibility applied under the Australian Privacy Act remains with the University therefore these obligations must be considered when entering into arrangements that permits access to sensitive and/or secure information with a third-party (e.g. vendor support, contractors, associated organisations).
18. Procedures to ensure the confidentiality, integrity and availability of information should be considered in conjunction with, but not limited to the following recommendations in respect to the information lifecycle:

Collection	<ul style="list-style-type: none"> • The source of information should be considered prior to making decisions (labelling, etc.) based upon its confidentiality or integrity: <ul style="list-style-type: none"> • Low: received from an unreliable source and has not yet been confirmed • Medium: received from associated organisation, validated and confirmed • High: received from a reliable source that has been confirmed • Collection of information is covered by the University Privacy Policy/Statement and can only be used for its intended purpose. • Aggregated data may result in an information classification higher than the individual data. E.g. UserID (public), Password (Public), UserID/Password (Secure) • Data volume may also require information classified at a higher level than individual data. e.g. 1 UserID/Password (Sensitive), Multiple UserID/Password (Secure)
Storage	<ul style="list-style-type: none"> • Clear Desk Standard: This organisation advocates a clear desk and screen policy particularly when employees are absent from their normal desk and outside normal working hours. In addition, screens on which confidential or sensitive information is processed or viewed should be sited in such a way that they cannot be viewed by unauthorised persons. Secure in lockable container, or at least lock office when unattended. • Password protected screen saver and/or always lock workstation when unattended • Computer Access Controls: password protect sensitive information, encrypt secure information. • Segregation of duties. • Operating procedures for handling of computer media (tapes, disks, diskettes, printouts, system logs) and system documentation.
Use	<ul style="list-style-type: none"> • Approval and authorisation of access by information Corporate Executive Portfolio Steward/System Principal Activity Steward/System Sponsor • Annual confidentiality agreement procedure • Privacy Statements • Access audit
Transmission	<ul style="list-style-type: none"> • Post: Certified mail, signed receipt or confirmation required for secure information. • Facsimile: Require phone call to receiving party before transmission, advised when message received. • Network transmission: Consider SSL (Secure Socket Layer) for sensitive information, required for secure information. • Web-accessibility: Only necessary information should be made available.
Disposal	<ul style="list-style-type: none"> • Paper: sensitive information should be shredded; secure information disposed using secure disposal service and consider shredding in addition before disposal. • Computer Disk: containing sensitive information should be re-formatted at least twice, secure information consider using commercial programs or service to wipe information off the media in a more secure manner.

3.1 Information Asset Security Classification Controls

The following Information Asset Security Classification Controls are based upon those outlined in the Queensland Government Information Security Classification.

3.1.1 Public

	Refer to Schema for Unclassified
Collection	
Storage	
Use	
Transmission	
Disposal	

3.1.2 Unclassified

	<p>UNCLASSIFIED information is official information that is not in the public domain, but does not otherwise need to be classified.</p> <p>UNCLASSIFIED information is information which still needs to be protected and controlled, and is not to be considered PUBLIC information. Official information needs to be specifically classified as PUBLIC before it is released. It may be helpful to mark information with this classification level so that it is known that the assessment has been made. Information which has not been assessed is best marked Not-Yet-Security-Assessed or with some similar identification and should be treated as UNCLASSIFIED.</p> <p>UNCLASSIFIED information may be marked as INTERNAL-USE-ONLY, UNIVERSITY-USE-ONLY or UNCLASSIFIED.</p>
Collection	<p>Preparation and Handling</p> <p><i>Markings</i> Not required, though helpful in distinguishing UNCLASSIFIED information from information that has not been classified.</p> <p><i>Page Numbering</i> Optional, but generally helpful.</p> <p><i>Filing:</i> File in accord with normal records management practices.</p> <p><i>User Auditing</i> Log in, log out, failed attempt.</p> <p><i>Printing</i> No special requirements.</p>
Storage	<p>Copying and storage</p> <p><i>Copying</i> To be kept to a minimum in accord with operational requirements.</p> <p><i>Storage</i> May be stored in unsecured compactus or cabinet.</p> <p><i>Electronic Storage</i> Common access drive or directory.</p>
Use	<p>Removal from workplace, and monitoring Removal of file or document only on a basis of need. Monitoring None required.</p> <p>Discussing Unclassified Information</p> <p><i>Meetings</i> No restriction but basis of 'need-to-know'</p> <p><i>Telephone and video conference</i> May be passed in the clear (unencrypted) over communications systems.</p>
Transmission	<p>Manual Transmission</p> <p><i>Within a single location</i> May be passed uncovered by hand. Passed by internal mail in a use again envelope.</p> <p><i>Between locations</i> Passed by internal mail in a use-gain envelope. Passed by external mail in an opaque envelope.</p> <p>Electronic Transmission</p> <p><i>Data transmission</i> Basis of 'need-to-know'. May be passed by data transfer using internal or external networks including the internet.</p> <p><i>email</i> Basis of 'need-to-know'. May be passed by email using internal or external</p>

	<p>networks including the internet.</p> <p><i>Fax</i></p> <p>Unclassified information may be passed in the clear (unencrypted) by fax.</p>
Disposal	<p>Archive & Disposal</p> <p>In accordance with authorised retention and disposal schedule issued under the <i>USQ Records Disposal Policy</i>.</p> <p><i>Paper waste</i></p> <p>Drafts, working papers and copies may be recycled.</p> <p>Drafts, working papers and copies may be discarded with general paper waste.</p> <p><i>Electronic Media & equipment</i></p> <p>Media may be reused or disposed of as per paper waste.</p>

3.1.3 Classified - Secure

	<p>Information whose compromise could cause damage to the University, commercial entities or members of the public. For instance, compromise could:</p> <ul style="list-style-type: none"> • endanger individuals and private entities; • work substantially against University finances or economic and commercial interests; • substantially undermine the financial viability of major organisations; or • seriously impede the development or operation of major University policies. <p>As a principle, most non-national security information would be adequately protected by the procedures given to information marked X-IN-CONFIDENCE or PROTECTED.</p>
Collection	<p>Preparation and Handling</p> <p><i>Markings</i> Distinct markings on document or information asset. Centre of top and bottom of each page, in capitals, 5mm (20 point) bold and red if possible.</p> <p><i>Page Numbering</i> Desirable.</p> <p><i>Filing</i> File in distinctive file (green). Appropriate file cover sheet to be used.</p> <p><i>Preparation of Electronic Information</i> Prepare in drive or electronic document and records management system with restricted access.</p> <p><i>User Auditing</i> Log in/out, failed attempt, Read, Write and Delete.</p> <p><i>Printing</i> Printer not to be left unattended while PROTECTED documents are being printed.</p>
Storage	<p>Copying and storage</p> <p><i>Copying</i> May be prohibited by information owner. To be kept to a minimum in accord with operational requirements.</p> <p><i>Physical Storage</i> 'Clear Desk' policy. Key lockable steel container (C-Class) in a secure or partially secure environment. Steel-lined, tamper-evident container with a combination lock (B-Class) in an intruder resistant environment.</p> <p><i>Electronic Information Storage</i> Restrict logical access based on need-to-know.</p>
Use	<p>Removal from workplace, and monitoring</p> <p><i>Removal of file or document</i> Basis of need. Authorisation of information owner required. Kept in personal custody. Ensure adequate storage arrangements.</p> <p><i>Monitoring</i> Regular checks of the Security Classified Information Register and information is desirable.</p> <p>Discussing Classified Information</p> <p><i>Meetings</i> Must occur behind closed doors in fully enclosed rooms. Notify classification to audience. Material must include classification markings. Remove from equipment and whiteboards prior to vacating room</p>

	<p><i>Telephone and video conference</i></p> <p>Telephone and video conference should not be used for data or voice transmission of material unless both ends are provided with encryption. Cordless or mobile phones should not be used to discuss protected information unless the security they use has been approved for this classification.</p>
Transmission	<p>Manual Transmission</p> <p><i>Within a single location</i></p> <p>Single opaque envelope indicating classification. Uncovered by hand directly between authorised members of staff in discrete office environment. Should not be left unattended on recipient's desk.</p> <p><i>Between locations</i></p> <p>Double enveloping (i.e. sealed inner envelope indicating classification placed within a single opaque outer envelope that does not indicate classification); or Single opaque envelope that does indicate classification and secured in a lockable container and delivered by an authorised messenger. Receipting required.</p> <p>Electronic Transmission</p> <p><i>Data transmission</i></p> <p>Basis of 'need-to-know'. May be passed over appropriately classified internal networks. Information should be encrypted when being sent between agencies using Transport Layer Security (TLS), Secure Sockets Layer (SSL) or IP Security (IPSec) encryption.</p> <p><i>eMail</i></p> <p>Basis of 'need-to-know'. May be passed over appropriately classified internal networks. Information must be encrypted (eg via secure email) when sent between agencies.</p> <p><i>Fax</i></p> <p>Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. Encrypted communications systems must be used to transmit PROTECTED information.</p>
Disposal	<p>Archive & Disposal</p> <p>In accordance with authorised retention and disposal schedule issued under the <i>USQ Records Disposal Policy</i>.</p> <p><i>Paper waste</i></p> <p>Drafts, working papers and copies must be shredded.</p> <p><i>Electronic Media & equipment</i></p> <p>Media to be destroyed or sanitised.</p>

3.1.4 Classified - Sensitive

	<p>Information whose compromise could cause limited damage to the University, commercial entities or members of the public, including:</p> <ul style="list-style-type: none"> • cause distress to individuals or private entities; • cause financial loss or loss of earning potential to, or facilitate improper gain or advantage for, individuals or private entities; • prejudice the investigation or facilitate the commission of crime; • breach undertakings to maintain the confidentiality of information provided by third parties; • impede the effective development or operation of University policies; • breach statutory restrictions on the management and disclosure of information; • disadvantage the University in commercial or policy negotiations with others; <p>or</p> <ul style="list-style-type: none"> • undermine the proper management of the University and its operations. <p>This protective marking is accompanied by a notification of the subject matter which alludes to its audience and the need-to-know principle. Examples include:</p> <p>STAFF-IN-CONFIDENCE, Includes all official staff records where access would be restricted to HR personnel and nominated authorised staff. For example, personal files, recruitment information, grievance or disciplinary records.</p> <p>EXECUTIVE-IN-CONFIDENCE Information associated with executive management of the entity that would normally be restricted to the executive and nominated authorised staff. For example, sensitive financial reports, strategic plans, University matters, Staff matters, etc.</p> <p>COMMERCIAL-IN-CONFIDENCE Procurement/contract or other commercial information such as sensitive intellectual property. For example, draft request for offer information, tender responses, tender evaluation records, designs and government owned research.</p> <p>AUDIT-IN-CONFIDENCE Information related to audit activities where access would be restricted to officers of the Audit department or nominated authorised staff. For example, Audit and Risk reports which identify security and control weaknesses.</p>
Collection	<p>Preparation and Handling</p> <p><i>Markings</i> Distinct markings on document or information asset. Centre of top and bottom of each page, in capitals, 5mm (20 point) bold and red if possible.</p> <p><i>Page Numbering</i> Desirable.</p> <p><i>Filing</i>: File in distinctive file (blue). Appropriate file cover sheet to be used.</p> <p><i>Preparation of Electronic Information</i> Prepare in drive or electronic document and records management system with restricted access.</p> <p><i>SCI Register</i> Desirable.</p> <p><i>User Auditing</i> Log in/out, failed attempt and Delete.</p> <p><i>Printing</i> Unless otherwise secured, Printer not to be left unattended.</p>
Storage	<p>Copying and storage</p> <p><i>Copying</i> May be prohibited by information owner. To be kept to a minimum in accord with operational requirements.</p> <p><i>Physical Storage</i></p>

	<p>'Clear Desk' policy. Lockable cabinet. <i>Electronic Information Storage</i> Restrict logical access based on need-to-know.</p>
Use	<p>Removal from workplace, and monitoring <i>Removal of file or document</i> Basis of need. Authorisation of information owner required. Kept in personal custody. Ensure adequate storage arrangements. <i>Monitoring</i> Basic checks only, no need for formal audit.</p> <p>Discussing Classified Information <i>Meetings</i> If discussions are held, care should be taken to ensure that people without a need to know are not able to overhear the discussions. If a meeting is held, Remove from equipment and whiteboards prior to vacating room. <i>Telephone and video conference</i> May be passed in the clear (unencrypted) over internal communications systems. Between sites, encryption is desirable but not mandatory.</p>
Transmission	<p>Manual Transmission <i>Within a single location</i> Single opaque envelope indicating classification. Uncovered by hand in discrete office environment. <i>Between locations</i> Single opaque envelope that does not indicate classification. Receiving at discretion of information owner. Delivered by hand or authorised messenger including Australia Post.</p> <p>Electronic Transmission <i>Data transmission</i> Basis of 'need-to-know'. May be passed unencrypted over appropriately classified internal networks. Information should be encrypted when being sent between agencies. <i>Email</i> Basis of 'need-to-know'. May be passed unencrypted over appropriately classified internal networks. Information should be encrypted (eg via secure email) when sent between agencies. <i>Fax</i> Required that someone attend the receiving facsimile to receive the material, and that receipt or non-receipt of the document is advised. Encryption is desirable but not mandatory</p>
Disposal	<p>Archive & Disposal In accordance with authorised retention and disposal schedule issued under the USQ Records Disposal Policy. <i>Paper waste</i> Drafts, working papers and copies may be recycled through lockable classified waste bins. Drafts, working papers and copies may also be shredded. <i>Electronic Media & equipment</i> Media may be reused or disposed of as per paper waste.</p>

	Collection	Storage	Use	Transmission	Disposal
Public	What we must do				
Unclassified					
Classified – Secure					
Classified - Sensitive					

4 Related Documents

Document (Electronic)	Business Classification Scheme Policy available at http://www.usq.edu.au/resources/116.pdf
Document (Electronic)	Business Classification Scheme – Level 1 Functions available at http://www.usq.edu.au/resources/1161.pdf
Document (Electronic)	Business Classification Scheme – Level 1 Functions (Scope Notes) available at http://www.usq.edu.au/resources/1162.pdf
Document (Electronic)	Business Classification Scheme – Level 2 Functions and Activities available at http://www.usq.edu.au/resources/1163.pdf
Document (Electronic)	Business Classification Scheme – Level 3 Functions, Activities and Transactions available at http://www.usq.edu.au/resources/1164.pdf
Document (Electronic)	Confidentiality Agreement template available at http://www.usq.edu.au/resources/1165.pdf
Document (Electronic)	ICT Standard for the Use of ICT Resources available at http://www.usq.edu.au/resources/ict_standard_for_the_use_of_ict_resources.pdf
Document (Electronic)	Qld. Govt. Information Security Classification Framework available at http://www.qgocio.qld.gov.au/02_infostand/downloads/qgiscf.doc
Document (Electronic)	USQ Archives Policy and Procedures available at http://www.usq.edu.au/resources/111.pdf
Document (Electronic)	USQ Records Disposal Policy available at http://www.usq.edu.au/resources/115.pdf