

INFORMATION ASSETS SECURITY CLASSIFICATION POLICY



CONTENTS

1	PURPOSE.....	1
2	SCOPE.....	1
3	POLICY STATEMENT	1
	Framework	1
	Implementation.....	3
4	RESPONSIBILITIES	4
	Compliance, monitoring and review.....	4
	Reporting.....	4
	Records management.....	4
5	DEFINITIONS	4
	Terms and definitions.....	4
6	RELATED LEGISLATION AND DOCUMENTS.....	4
7	FEEDBACK.....	5
8	APPROVAL AND REVIEW DETAILS.....	5

1 PURPOSE

- 1.1 This policy describes the approach to managing the security classification of information assets at CQUniversity, and outlines the standards by which information assets will be managed.

2 SCOPE

- 2.1 This policy applies to all CQUniversity information assets, including those involved in outbound and/or inbound information transfers.
- 2.2 This policy focuses specifically on the classification and control of non-national security information assets, and is primarily intended for the recognised officers responsible for:
- implementing and maintaining information assets
 - incorporating security, integrity, privacy, confidentiality, accessibility, quality and consistency, and
 - the specific classifications or categorisations of information assets.

3 POLICY STATEMENT

- 3.1 CQUniversity maintains a classification scheme and all information assets must be risk assessed, classified and protected according to this scheme based upon the type of asset and its sensitivity. All legal, regulatory and compliance requirements will be considered when determining classification levels.

Framework

- 3.2 For the purposes of classification, an information asset may consist of related information items, grouped together so that broadly similar controls may be applied to the group. Each significant information asset must be classified by the information asset owner based on the confidentiality, integrity and availability requirements of the most sensitive part and business valuable parts of the collection.
- 3.3 CQUniversity makes use of the [Queensland Government Information Security Classification Framework](#) (QGISCF). The following QGISCF classifications levels are used by CQUniversity:

Security Aspect	Classification	Information Type and Controls	
		Information	Controls
Confidentiality	Highly Protected	Information assets that require a substantial degree of protection as their compromise could cause serious damage to the University, the State, Government, commercial entities or members of the public.	Strict access controls e.g. strong encryption routines with long keys; biometric authentication; safes Electronic media must be destroyed or sanitized.
	Protected	Information assets whose compromise could cause damage to the University, the State, Government, commercial entities or members of the public. This level of classification also includes cabinet-in-confidence/sensitive cabinet.	Strict access controls e.g. strong encryption routines with long keys; biometric authentication; safes Electronic media must be destroyed or sanitized.
	Confidential (X-in-confidence)	Information assets whose compromise could cause limited damage to the University, the State, Government, commercial entities or members of the public. Examples include legal-in-confidence, commercial-in-confidence, and staff-in-confidence.	Strong access controls e.g. standard encryption routines and keys; multifactor authentication; locked filing cabinets.
	Unclassified	Information assets that do not need special security controls or require a classification level. These are not in the public domain, but do not otherwise need to be classified. These information assets require approval from the information owner to be released to the public.	Routine access controls as per Information Security Policies.
	Public	Information assets which have been authorised by the owner for public access and circulation, such as agency publications or on web sites.	No specific requirement.
Integrity	High Integrity	Important financial, operational or safety information.	Strict data validation, automated periodic system integrity checks
	Medium Integrity	Routine operational information	Routine data validation, manual system integrity checks
	Low Integrity	General low value business information (easily recreated)	No specific requirement.
Availability	Tier 1	Important financial, operational or safety information.	“Live-live” or equivalent highly resilient systems and proven disaster recovery arrangements
	Tier 2	Information used routinely	Cold standby disaster recovery arrangements.
	Tier 3	Supplementary/Low value Information	No specific requirement

Implementation

- 3.4 The University shall ensure that all employees have a clear understanding of the Information Classification scheme and its requirements.
- 3.5 All University information assets must be accounted for and have a designated information asset owner. These assets are stored in the Information Assets Register.
- 3.6 Ownership of existing University information assets must be determined by the responsible division.
- 3.7 It is the responsibility of the information asset owner to:
 - define the information assets
 - ensure they are classified according to the scheme, and
 - to periodically review the classification of the asset and verify it is kept current.
- 3.8 In the event that an information asset cannot be classified, it will be reviewed by the Information and Technology and Governance Directorates to ensure that appropriate access and protections are implemented.
- 3.9 Information asset owners will only provide access to authorised individuals who have a legitimate need to access that information to fulfil their official duties or contractual responsibilities.
- 3.10 System administrators (custodians) responsible for the protection of information assets will ensure access is limited based on the requirements of the [Information Security Management Policy and Procedure \(FMPM\)](#) and specifically the Information Access Control section.
- 3.11 It is the responsibility of authorised individuals granted access to ensure that the information assets are handled with due care and protected according to its security classification, as required by CQUniversity policies, procedures and legislative requirements.
- 3.12 The University will perform periodic reviews of classified information to ensure that users with access are appropriate and approved by information owners.
- 3.13 When information assets of various information security classifications are combined, the resulting data collection must be classified at the most restricted level within the data collection.
- 3.14 Data retention will be determined by the information asset owner and limited to the least amount of time taking into account all legal, regulatory and compliance requirements.
- 3.15 Information assets will be destroyed/purged based upon retention schedules. Where possible, data purge will be automated.
- 3.16 Information encryption will be implemented for sensitive information both at rest and in motion as required by information security policies and any legal, regulatory or compliance entity.
- 3.17 Sensitive information must only be released in accordance with the University policies, legislative requirements and directives of the Government and Courts of Law.
- 3.18 Sensitive and proprietary information will not be shared with third parties unless explicitly approved by the information asset owner and/or the Information and Technology Directorate.
- 3.19 Production data containing sensitive information will not be used in development or quality assurance environments without appropriate de-identification, masking or redaction of the sensitive information.
- 3.20 All devices and applications that interact with sensitive data shall have a method of logging the user/system activity back to the account used to access the data. Any unauthorized access will be researched to determine if access was appropriate or if data was compromised.
- 3.21 All new information assets must be evaluated against the [QGISCF](#) during their acquisition or creation.

- 3.22 Existing information assets must be evaluated when process changes occur to the collection or storage of the information, such as during the implementation of a new records or document management process or a new information system. A particular driver for an implementation or review of security classification would be the implementation of a new process or system which enables the transfer of information within and beyond the University's boundaries.

4 RESPONSIBILITIES

Compliance, monitoring and review

- 4.1 The Chief Information and Digital Officer is responsible for ensuring the implementation of this policy and the upkeep of the Information Assets Register.
- 4.2 Information assets are owned by CQUniversity, and individuals are assigned and made accountable for the management, custodianship and operational support of information assets. Information assets owners, information custodians and managers of information assets are responsible for undertaking periodic reviews and updating of details held in the Information Assets Register.
- 4.3 All existing information assets must be periodically reviewed and re-evaluated against the [QGISCF](#) based on an assessment of risk, with high risk information assets being considered a priority for evaluation. This review will usually occur in conjunction with the annual review of the Information Assets Register.

Reporting

- 4.4 No additional reporting is required.

Records management

- 4.5 Staff must maintain all records relevant to administering this policy in a recognised University recordkeeping system.

5 DEFINITIONS

- 5.1 Terms not defined in this document may be in the University [glossary](#).

Terms and definitions

Information asset: a body of information, defined and managed as a single unit, so that it can be understood, shared, protected and utilised effectively. Information assets have recognisable and manageable value, risk, content and lifecycles and enable the business to perform its functions, thereby satisfying a recognised business requirement.

Information asset owner: subject matter experts within the University who are responsible for ensuring that specific information assets are used and managed appropriately.

Non-national security information: information asset that requires increased protection and does not meet the definition of national security information.

6 RELATED LEGISLATION AND DOCUMENTS

[Queensland Government Information Asset Custodianship Policy \(IS44\)](#)

[Queensland Government Information Security Classification Framework \(QGISCF\)](#)

[Queensland Government Information Security Controls Standard](#)

[Queensland Government Information Security Information Standard \(IS18\)](#)

[Public Records Act 2002](#) (Qld)

The following documents are available on the [Information Asset Security page](#) in Staffnet (*available to employees only*)

- Information Asset Register
- Information Asset Owners Guide
- Information Assets – Secure Handling Guide

7 FEEDBACK

7.1 University staff and students may provide feedback about this document by emailing policy@cqu.edu.au.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Vice-Chancellor and President
Advisory Committee to Approval Authority	Vice-Chancellor's Advisory Committee
Administrator	Chief Information and Digital Officer
Next Review Date	7/03/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Vice-Chancellor and President 11/09/2013
Amendment Authority and Date	Vice-Chancellor and President 9/11/2016; Vice-Chancellor and President 7/03/2018.
Notes	Formerly known as the Information Asset Classification Principles (11/09/2013).