INFORMATION SECURITY MANAGEMENT POLICY

CONTENTS

1 PURPOSE

1.1 CQUniversity is committed to managing information security in accordance with University policies and relevant laws and regulations.

1.2 This policy outlines how CQUniversity will manage and mitigate security risks to safeguard the confidentiality, integrity and availability of University information and communication technology assets and environment.

2 SCOPE

2.1 This policy applies to the University as a corporate entity, members of the University Council and the University Council as whole, employees (regardless of their mode of employment) of CQUniversity and its controlled entities. This policy also applies to contractors, service providers and other members of the University’s supply chain who are provided access to the University systems or data as required to deliver contracted services.

3 POLICY STATEMENT

3.1 CQUniversity is committed to the secure management of information and systems utilising a policy framework based on the international standard for security management systems - ISO 27001, as required by the Queensland Government Chief Information Office (QGCIO) Information Security Standard IS18. The University will manage information security risks and controls to the extent that there are clear financial benefits to the University. Where the cost of control does not present an advantage over the potential cost of risk, a deviation from IS18 may be considered.

Information security principles

3.2 CQUniversity has adopted the following high-level Information security principles to establish a sound foundation for information security policies, procedures and practices. These principles are:

- Information, in whatever form, is of fundamental importance to the University and as such the University will manage information security within a framework based on ISO 27001.

- Information security risks will be managed, taking into account broader University objectives, strategies and priorities. A risk management approach will be used to identify, evaluate and mitigate risks for the University's systems and information assets. This is supported by the Risk Management Policy and Procedure (FMPM) and related risk management information.
- The requirements of the ISO 27001 Standard, the QGCIO, and therefore this policy are based on the following three elements of information security:
  - Confidentiality: ensuring that information will be accessible only to those authorised to have access
  - Integrity: safeguarding the accuracy and completeness of information and processing methods, and
  - Availability: ensuring that authorised users will have access to information and associated assets when required.
- CQUniversity's management will actively support information security within the organisational culture through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities. This will ensure information security management is embedded in University activities and processes.
- Continuity of operations will be heavily dependent upon the confidentiality, integrity and continued availability of information and the means by which it is gathered, stored and processed, communicated and reported. This is supported by the Information Assets Security Classification Policy.

Supporting policy domains

3.3 This policy has defined 15 policy domains aligned with ISO 27001:2013 as listed below. These domains are subject areas in which management controls are defined, applied and governed by one or more local Information and Technology Directorate documents and are contained in the Information Security Management System (ISMS). The following table describes these domains.

Policy Domain	Summary
Information Security Management System (ISMS)	The ISMS provides the framework of principles, policies, standards and guidelines for the effective management of IT Security Risk.
Access controls	Methods and controls to manage logical access to sensitive data to protect confidentiality of information as well as integrity and availability requirements. Access requirements are assessed against the Queensland Government Authentication Framework and the Information Assets Security Classification Policy. Access to University information and systems must be: • attributable to a uniquely identifiable individual who is responsible for actions performed with their system account • based on the requirements of the individual's role • managed by passwords, according to Information and Communication Technology Passwords Procedure, formally authorised by asset owners, routinely revalidated and removed if no longer required
Communications Security	Methods and controls to manage the secure transmission of information to ensure confidentiality of sensitive data and to minimise the risk of data loss or leakage. Systems and networks will be segregated according to their respective information security risks and use appropriate control mechanisms such as firewalls/gateways, physical isolation and encryption.
Operations Security	Methods and controls that balance the need for IT Operations professionals to have privileged access to systems and networks with the requirement to maintain secure access and confidentiality of data. Management and operation of computers and networks shall be, commensurate with the business risk and value of the information assets. Access into networks will be granted on an individual user and application basis using authorised devices and secured pathways.

Physical and Environmental Security	Appropriate physical controls will protect information assets against loss, physical abuse, unauthorised access and environmental hazards. These will include perimeter security controls, physical access controls, intruder detection controls, fire, and flood and power protection controls.
Supplier Relationships	The University will implement security controls and processes to manage supplier access to information assets. Suppliers and vendors will be given access privileges only at the level required to deliver contracted services and contracts must comply with information security policies.
Systems Acquisition and Secure Development	Information security controls will be specified and included as an integral part of the software development and implementation process. Security requirements will be identified prior to the development or procurement of IT systems, documented in business requirements, validated and tested prior to implementation, and regularly throughout the systems lifecycle.
Cryptography	Methods and controls for ensuring data will be secured during transmission, or storage through appropriate encryption processes. Includes methods and processes for managing keys, software and other artefacts.
Incident Management	The University will apply a consistent and effective approach to the management of information security incidents. Procedures that define the course of action when a security incident is identified will be documented and made available to all employees.
Business Continuity	The application of business continuity management shall minimise disruption to CQU operations, defining the approach to resilience, disaster recovery and general contingency controls. Continuity plans shall align with the University's Business Continuity Management Framework.
Human Resources	The University will establish processes and responsibilities relating to information security during the recruitment process, employment and separation. Security checks will be conducted prior to employment and all employees will receive security awareness training upon induction, and at least annually thereafter.
Project Management	Project proposals must include a high-level risk assessment and review of the types and confidentiality levels of information the project will utilise and manage. New systems will be reviewed by the Information Security Officer prior to implementation via the change management process.
Asset Management	IT assets, including hardware, software and data will be identified and classified and asset inventories will be maintained. The University will classify and handle all information assets in accordance with the Queensland Government Information Security Classification Framework (Section 2). The University will dispose of public records in accordance with the University's Retention and Disposal Schedules, as approved by the State Archivist, or in accordance with the *Public Records Act 2002* (Qld).
Data Assurance	The University will ensure that all reasonable steps are taken to monitor, review and audit information security effectiveness. This will include the assignment of security roles, maintenance of policies and processes and reporting of non-compliance.
Data Breach Reporting	The University has formal processes in place to manage a data breach and the mandatory notifications that are required under the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cwlth).

4 RESPONSIBILITIES

Compliance, monitoring and review

4.1 The Chief Information and Digital Officer is responsible for monitoring, reviewing and ensuring compliance with this policy.

Reporting

4.2 Individual responsibility for implementation of components of this policy will be allocated to the Deputy Director, Digital Information.

Records management

4.3 Staff must maintain all records relevant to administering this policy and procedure 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 Security Management System (ISMS): a systematic approach to managing sensitive University information so that it remains secure. It includes people, processes and IT systems by applying a risk management process.

Information Security Supporting Principles: a set of principles that the policy domains described in section 3.3. This is located on a StaffNet (*available to employees only*).

6 RELATED LEGISLATION AND DOCUMENTS

Australian Standards:

- AS/NZS ISO/IEC 27001 Information technology -- Security techniques –Information security management systems
- AS/NZS ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security management

Information and Communications Technology Passwords Procedure

Information Assets Security Classification Policy

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cwlth)

Queensland Government Information Standards

- IS 13: Procurement and Disposal of ICT Products and Services
- IS 18: Information Security
- IS 31: Retention and Disposal of Public Records
- IS 33: Information Access and Use
- IS 38: Use of ICT Facilities and Devices
- IS 40: Recordkeeping
- IS 44: Information Asset Custodianship

Risk Management Policy and Procedure (FMPM)

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	13/06/2021

Approval and Amendment History	Details
Original Approval Authority and Date	Council 01/05/2007
Amendment Authority and Date	Updated 27/03/2015 to include references to the Information Security Strategy. Updated on 14/09/2009; Director IT approved changes to Governance and procedures 10/03/2010; Vice-Chancellor and President 29/11/2010 Vice-Chancellor and President 13/05/2015; Vice-Chancellor and President 6/06/2018.
Notes	This document was formerly known as the Information Security Management Policy and Procedure (FMPM) (13/05/2015).