CYBERSECURITY MANAGEMENT POLICY

CONTENTS

1 PURPOSE

1.1 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
- employees, students, and Council and Committee members of CQUniversity and its controlled entities, and
- other individuals working on the University's behalf or using University-owned information and communication technology (ICT) resources including 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 The University is committed to managing cybersecurity in accordance with University policy documents and relevant laws and regulations, and to the secure management of information and systems utilising a policy framework based on the international standard for security management systems (ISO/IEC 27001:2022), as required by the Queensland Government Enterprise Architecture (QGEA) Information Security Policy (IS18:2018). The University will manage cybersecurity 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 the Information Security Policy (IS18:2018) may be considered.

Cybersecurity principles

3.2 The University has adopted the following high-level cybersecurity principles to establish a sound foundation for cybersecurity 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 cybersecurity within a framework based on the internationally recognised information security management system standard ISO/IEC 27001:2022.
- Cybersecurity 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 Enterprise Risk Management Framework and related risk management information.
- The requirements of the international information security management system standard ISO/IEC 27001:2022, the Queensland Government Enterprise Architecture, and therefore this policy, are based on the following three elements of cybersecurity:
    - 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.
- Management will actively support cybersecurity within the organisational culture through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of cybersecurity responsibilities. This will ensure cybersecurity 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 the international information security management system standard ISO/IEC 27001:2022 as listed below. These domains are subject areas in which management controls are defined, applied and governed by one or more local Digital Services Directorate documents and are contained in the Information Security Management System. The following table describes these domains.

Policy Domain	Summary
Information Security Management System	The Information Security Management System provides the framework of principles, policies, standards and guidelines for the effective management of information and communications technology 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 • authorised formally by asset owners, routinely revalidated, removed if no longer required, and managed by passwords and multifactor authentication (MFA) according to the Information and Communications Technology Passwords Procedure.
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 cybersecurity risks and use appropriate control mechanisms such as firewalls, gateways, physical isolation, and encryption.

Operations Security	Methods and controls that balance the need for information and communications technology 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 will 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 protection controls, flood protection controls, 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 cybersecurity policy documents.
Systems Acquisition and Secure Development	Cybersecurity 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 information and communication technology 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 cybersecurity incidents. Procedures that define the course of action when a cybersecurity incident is identified will be documented and made available to all employees.
Business Continuity	The application of business continuity management will minimise disruption to University operations, defining the approach to resilience, disaster recovery and general contingency controls. Continuity plans will align with the University's Business Continuity Planning and Incident Management Policy and Procedure.
Human Resources	The University will establish processes and responsibilities relating to cybersecurity during the recruitment process, employment and separation. Security checks will be conducted prior to employment. All employees will receive cybersecurity 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 a Cybersecurity Officer prior to implementation via the change management process.
Asset Management	Information and communication technology 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 relevant Retention and Disposal Schedule, as or in accordance with the *Public Records Act 2002* (Qld). Refer to the Records Management Policy and Procedure on the process for disposing records.
Data Assurance	The University will ensure that all reasonable steps are taken to monitor, review and audit cybersecurity effectiveness. This will include the assignment of cybersecurity 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 Digital Officer is responsible for implementing, monitoring, reviewing and ensuring compliance with this policy.

4.2 Individual responsibility for implementation of components of this policy will be allocated to the Director Data and Cybersecurity.

Reporting

4.3 No additional reporting is required.

Records management

4.4 Employees must manage records in accordance with the Records Management Policy and Procedure. This includes retaining these records in a recognised University recordkeeping information system.

4.5 University records must be retained for the minimum periods specified in the relevant Retention and Disposal Schedule. Before disposing of any records, approval must be sought from the Records and Privacy Team (email records@cqu.edu.au).

5 DEFINITIONS

5.1 Terms not defined in this document may be in the University glossary.

Terms and definitions

Employee: any person employed by CQUniversity or its controlled entities on a permanent, fixed-term or casual basis.

Information Security Management System: a systematic approach to managing sensitive University information so that it remains secure. It includes people, processes and information and communication technology systems by applying a risk management process.

6 RELATED LEGISLATION AND DOCUMENTS

Australian Standard – AS/NZS ISO/IEC 27001:2023 Information security, cybersecurity and privacy protection - information security management systems – requirements

Australian Standard - AS/NZS ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – information security controls

Business Continuity Planning and Incident Management Policy and Procedure

Enterprise Risk Management Framework

Information Access and Use Policy (IS33) (Queensland Government Enterprise Architecture)

Information and Communications Technology Passwords Procedure

Information Asset Custodianship Policy (IS44) (Queensland Government Enterprise Architecture)

Information Assets Security Classification Policy

Information Security Policy (IS18:2018) (Queensland Government Enterprise Architecture)

International Standard - ISO/IEC 27001:2022 Information security management system

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

Procurement and Disposal of ICT Products and Services Policy (IS13) (Queensland Government Enterprise Architecture)

Queensland Government Authentication Framework (Queensland Government Enterprise Architecture)

Queensland Government Information Security Classification Framework (Queensland Government Enterprise Architecture)

Records Governance Policy (Queensland Government Enterprise Architecture)

Risk Management Policy

Use of ICT Services, Facilities and Devices Policy (IS38) (Queensland Government Enterprise Architecture)

7 FEEDBACK

7.1 Feedback about this document can be emailed to policy@cqu.edu.au.

8 APPROVAL AND REVIEW DETAILS

Approval and Review	Details
Approval Authority	Vice-Chancellor and President
Delegated Approval Authority	Chief Operating Officer
Advisory Committee	N/A
Required Consultation	N/A
Administrator	Chief Digital Officer
Next Review Date	17/12/2024

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; Deputy Vice-President (Digital Services) 14/09/2020; Editorial amendment 19/01/2021; Deputy Vice-President (Digital Services) 17/12/2021; Editorial amendments 05/01/2023; Editorial amendments 08/02/2023; Editorial amendments 07/02/2024.
Notes	This document consolidated and replaced the Information Security Policy and Information Security Procedure (11/03/2010), Information Security Management Policy and Information Security Management Principles (29/11/2010) and the Information Security Management Policy and Procedure (13/05/2015). This document was formerly known as the Information Security Management Policy and Procedure (06/06/2018).