Cyber Security Policy

Section 1 - Purpose and Scope

(1) Cyber security enables confidentiality, integrity and availability of information by providing protection against malicious and accidental threats. Cyber security threats take advantage of weaknesses in technology, people and processes to harm information. The University of Queensland (UQ or the University) manages cyber security risk to safeguard its mission and protect the interests of the people whose personal information it holds.

(2) This Policy establishes UQ's cyber security risk management and responsibilities, and is based on the principle that 'cyber security is everyone's business'. Management of cyber security risk requires a concerted effort across all of UQ and cannot be considered just an aspect of information technology.

(3) UQ's approach to cyber security is informed by the Queensland Government Information and Cyber Security Policy (IS18) (IS18:2018).

Scope

(4) This Policy is broad and applies to parties at UQ that hold or process UQ information, including:

a. Students;
b. Staff;
c. Third parties (e.g. suppliers, contractors, consultants and partners); and
d. Visitors.

(5) Consumers using UQ networks or services must comply with this Policy, irrespective of location or device ownership (e.g. consumers with personally owned computers). Exceptions to this Policy must be approved by the Chief Information Officer.

Section 2 - Principles and Key Requirements

Information Security Management Systems (ISMS)

(6) UQ's ISMS supports the Cyber Security Strategy, which seeks to mitigate risk and protect UQ's critical information against increasingly aggressive and sophisticated cyber threats whilst continually adapting to UQ's rapidly evolving needs. The key components of the ISMS are:

a. A Cyber Security Framework comprised of policies, procedures, local operating procedures, standards, guidelines and systems governing and facilitating cyber security management at UQ.
b. Technical cyber security controls to protect information systems.
c. A cyber security awareness program to reduce the vulnerability of staff and students to cyber security threats and foster a culture that facilitates cyber security.

Cyber Security Framework

(7) The key platforms of the framework are information management, cyber security risk management and cyber security incident management, as explained below.

a. The specification of cyber security controls is incorporated into relevant IT standards or as separate cyber security standards.
b. The University will have sufficient IT and cyber security standards to facilitate the effective implementation of cyber security controls across all IT infrastructure, systems and applications.
c. Standards will be developed in consultation with key stakeholders to support business requirements, provide adequate cyber security risk mitigation, and align with the cyber security strategy.
d. The Cyber Security Exceptions Procedure is available for instances where the standard is not suitable, otherwise the standard must be followed.
e. Standards will be updated as required to reflect changes in security controls.

Information Management

(8) Information management is critical to robust cyber security. Underpinning the cyber security framework, UQ's Information Management Framework facilitates identification, management and governance of information assets. It mandates the security classification of information assets which provides the basis for consistent, risk-based protection.

(9) Systems storing or processing UQ information must meet the minimum technical controls outlined in the Application Security Controls Standard. Where a system is external to UQ (hosted by a third party), it is the responsibility of the Contract Manager to ensure the system meets these standards.

Cyber Security Risk Management

(10) Cyber security controls seek to reduce cyber security risk by either reducing the likelihood or impact of an incident, or both. UQ will continue to identify and treat cyber security risk via the following measures:

a. maintaining a register of key information assets;
b. establishing a framework for performing cyber security risk assessments aligned with UQ's Enterprise Risk Management Framework;
c. incorporating cyber security risk identification and assessment into processes impacting the use and processing of UQ information;
d. maintaining a register of cyber security risks with related controls;
e. reviewing risks at regular intervals and as a result of significant security incidents, threats or changes to business requirements;
f. implementing and strengthening controls to reduce risk; and
g. evaluating the effectiveness of controls.

Cyber Security Incident Management

(11) A cyber security incident is an event involving an actual or potential malicious actor that threatens the confidentiality, integrity or availability of UQ information assets (electronic or paper) or otherwise contravenes the University's Cyber Security Policy (this Policy). The source of a cyber security incident may be accidental, malicious or significant exposure to a known threat.

(12) The Cyber Security Incident Response Procedure details how incidents are managed and aims to comply with applicable legal requirements, minimise harm to impacted individuals, and minimise damage and risk to UQ.

(13) Incidents should be reported immediately to IT support.

Cyber Security Vulnerability Testing

(14) Security testing will be performed against systems, processes and people to determine UQ's vulnerability to cyber threats. The results of these test processes will only be used to measure and improve service quality and UQ's protection against cyber threats.

Section 3 - Roles, Responsibilities and Accountabilities

Consumers

(15) Consumers are responsible for reporting potential cyber security incidents to IT support, including those of an accidental nature such as a lost laptop or device.

(16) UQ staff and contractors are responsible for:

a. Participating in cyber security training where relevant to their work role; and
b. Acting consistently and responsibly to protect the University's information assets by:
    i. complying with procedures in place to protect information assets;
    ii. incorporating safe cyber security practices into their work; and
    iii. reporting risks to IT support.

IT Management and Staff

(17) IT managers manage relevant cyber security risks and are accountable for compliance with relevant cyber security standards.

(18) IT staff are responsible for:

a. Complying with relevant IT and cyber security standards and local operating procedures.
b. Assisting the Chief Information Officer to identify and develop suitable cyber security frameworks, standards and local operating procedures.
c. Monitoring IT systems and services for potential cyber security risks and threats.

Security Architect

(19) The Security Architect is responsible for:

a. Facilitating, monitoring and supporting cyber security risk management and compliance practices.
b. Developing and maintaining cyber security strategy, policy, procedures, frameworks, local operating procedures and standards.
c. Incorporating cyber security into IT frameworks, local operating procedures and standards.
d. Overseeing the implementation and operation of UQ's cyber security controls with broad impact.
e. Providing cyber security risk management information, resources and training to consumers.

Chief Information Officer

(20) The Chief Information Officer is responsible for:

a. Promoting the importance of cyber security risk management to UQ leadership and staff delivering IT services.
b. Providing adequate resourcing for the management of cyber security risk.
c. Reporting on cyber security risk to the University Senior Management Group and Senate.

Information Technology Governance Committee (ITGC)

(21) The ITGC will approve cyber security procedures, local operating procedures, and standards.

Strategic Information Technology Council (SITC)

(22) The SITC provides guidance and governance of the provision and direction of University-wide information technology and cyber security strategy, reporting to the University Senior Management Group on these areas.

Enterprise Risk Services

(23) Enterprise Risk Services, within the Governance and Risk Division, facilitates the effective management of risk at UQ. It is responsible for providing the Enterprise Risk Management Framework and risk appetite statements for cyber security.

Contract Managers

(24) Unless otherwise stated in a contract or agreement with UQ, Contract Managers are responsible for ensuring suppliers or partners processing UQ information are:

a. Managing cyber security risk to protect UQ information.
b. Providing assurance to UQ about cyber security risk management activities.
c. Reporting to UQ any breaches impacting or potentially impacting UQ information as soon as practical after detection of the breach.

Section 4 - Monitoring, Review and Assurance

Ongoing Review

(25) The Chief Information Officer will review this Policy at least every three years to ensure it aligns with UQ's cyber security strategy and industry best practice.

(26) Information Technology Services will assess the ongoing maturity of UQ's cyber security practices and review this Policy in response to significant cyber security incidents and changes in UQ's cyber security strategy and applicable legislation.

(27) Information Technology Services will drive compliance with the Policy through:

a. ongoing cyber security awareness activities;
b. checks in key IT processes to ensure cyber security risk management activities are performed;
c. technical enforcement;
d. regular reporting of self-assessments by Organisational Units on required cyber security controls implemented to protect information assets; and
e. audits to assess compliance and effectiveness of technical controls.

Internal Audit

(28) Internal Audit will provide independent oversight, review and assurance on the effectiveness of cyber security controls to manage risk and meet compliance requirements.

Section 5 - Recording and Reporting

(29) The IT Security Architect is accountable for the maintenance of cyber security metrics for periodic reporting to stakeholders. The metrics will cover the following aspects of UQ's cyber security management:

a. Current risk level;
b. Control effectiveness;
c. Maturity of the University's approach to cyber security against best practice frameworks; and
d. Financial status.

(30) Quarterly cyber security reports will be provided to the Senate Risk and Audit Committee.

Mandatory Reporting of Private Data Breaches

(31) Under the Privacy Act 1988 (Cth), UQ must report to the Australian Information Commissioner breaches of certain private data likely to cause serious harm, unless remediation occurs before any serious harm results from the breach. In UQ's case, this is limited to breaches involving tax file numbers and metadata collected under the Telecommunications (Interception and Access) Act 1979 (Cth). Additional notification obligations may be imposed under contracts entered into by the University.

Section 6 - Appendix

Related Policies and Procedures

(32) Information Management Policy

(33) Cyber Security Incident Response Procedure

(34) Cyber Security Framework (UQ login required)

(35) Cyber Security Risk Management Procedure (UQ login required)

(36) Cyber Security Exceptions Procedure.

Status and Details

Status	Current
Effective Date	28th November 2019
Review Date	13th May 2022
Approval Authority	Vice-Chancellor and President
Approval Date	28th November 2019
Expiry Date	Not Applicable
Policy Owner	Zoran Sugarevski Chief Information Officer
Enquiries Contact	Information Technology Services