1.0 Purpose and Scope

The University of Queensland (UQ) is committed to providing Information and Communication Technology (ICT) resources to support, enable and enhance its activities.

This policy:

- Outlines acceptable use (and misuse) of UQ ICT resources
- Supports UQ through effective provisioning and management of ICT resources
- Seeks to protect UQ’s reputation and safeguard its resources.

This policy should be read in conjunction with other ICT policies and procedures.

1.1 Scope

This policy applies to consumers using UQ ICT resources or UQ information including, but not limited to:

a) Students
b) Staff
c) Contractors and consultants
d) Visitors
e) Affiliates and third parties

Consumers that are connected to UQ networks or services must comply with this policy, irrespective of location or device ownership (e.g. consumers with personally-owned computers). The Chief Information Officer (CIO) must approve exceptions to this policy.

2.0 Principles and Key Requirements

ICT is of critical importance to UQ activities. All consumers of UQ ICT resources are expected to use these facilities and services appropriately and reasonably.

2.1 Access to ICT Systems and Resources

Access to ICT systems and resources is provided to consumers for carrying out University work, study, or for other UQ purposes. UQ incurs costs in providing ICT systems and resources, and access is not provided to consumers unconditionally. The following conditions apply:

a) Consumers must not share account login details such as usernames or passwords.
b) Passwords must be secure in accordance with the Password Guidelines.
c) Staff access to UQ ICT systems and resources is terminated when employment with UQ ceases. Account access may be extended in some circumstances, as outlined in the Information and Communication Technology Procedure.
d) UQ reserves the right to suspend or remove access where necessary.
e) UQ will take appropriate steps to ensure Internet access is granted to minors in compliance with legislative requirements.

f) UQ will endeavour to make online services accessible in alignment with industry best practices and accessibility guidelines.

2.2 Software

Software licensed to UQ (UQ Licensed Software) must only be used for purposes legitimately associated with UQ’s operations as a teaching and research institution and in accordance with the relevant software licence terms. This includes online services (i.e. software-as-a-service) licensed to UQ.

The following conditions of use are intended to inform consumers of their responsibilities when using UQ Licensed Software and to minimise UQ’s risks of copyright infringement, or other breach of software licence terms:

a) All UQ Licensed Software will only be used in compliance with the applicable licence terms and conditions.

b) Consumers should be aware of and comply with the terms and conditions of any software that is being used.

c) Delegates identified within the Contractual Delegations Policy are the only individuals at UQ that are authorised to approve software agreements on behalf of the University.

d) Information and communication technology procedures outline roles and responsibilities of IT staff and consumers when purchasing and installing software.

e) UQ Licensed Software must not be installed on personally-owned devices, unless explicitly permitted in the applicable licensing agreement and by management. Consumers must not install software on UQ devices that is not appropriately licensed to UQ.

f) Installation files for UQ Licensed Software must not be unlawfully copied, and unlawfully copied software must not be used or installed on UQ devices.

g) UQ Licensed Software master media and licence keys (where applicable) will be securely stored in order to avoid theft or unauthorised use or copying.

2.3 Acceptable Use of ICT Resources

UQ requires all consumers of its ICT resources to do so in a responsible, ethical, equitable and legal manner and in accordance with the UQ Code of Conduct (PPL 1.50.01 Code of Conduct) and Student Charter. Incidental personal use of University ICT resources is permitted. Such use must be kept to a minimum.

While UQ acknowledges that exceptions may exist under certain circumstances, inappropriate use of ICT resources may lead to increased cost, risk, and reputational damage to UQ. Consumers should be aware that UQ ICT resources must not be used:

a) for gambling purposes

b) in a manner that constitutes an infringement of copyright.

c) to access, store or transmit pornographic, racist, violent, or any other unacceptable or harmful material.
2.4 Misuse of UQ ICT Resources

The Chief Information Officer may authorise an investigation into alleged misuse. If allegations are deemed to be valid and of a serious nature, evidence of misuse will be reported to the appropriate body:

- If the consumer is a staff member – formal disciplinary action will occur in accordance with the Misconduct/Serious Misconduct clauses as outlined in the Enterprise Agreement. The case may also be referred to the Integrity and Investigations Unit.
- If the consumer is a student – the information will be reported to Student Integrity and Misconduct in accordance with the Student Integrity and Misconduct Policy (PPL 3.60.04).

2.5 Email and Bulk Messaging

UQ recognises the importance of email for efficient communication. Inappropriate use of email can result in security risks and reputational damage. Consumers should be aware of the measures below.

a) Information Technology Services will maintain the official email system for UQ, whether it be provided internally or through an agreement with an external service provider.

b) If an Organisational Unit wishes to maintain its own email server, approval must be obtained from the Chief Information Officer.

c) A UQ email address must be used for the delivery of all official UQ email.

d) Staff must not use external email accounts (e.g. Gmail, BigPond, or Hotmail) for UQ correspondence.

e) Academic staff may be eligible to retain access to their email account when employment with UQ ceases. Accounts with no activity for a period of 6 months will be suspended.

f) Students, Alumni, volunteers, Academic Title Holders, and Honoraries may forward their UQ email to another account or provider. Staff email accounts must not be forwarded to an external provider without approval.

g) UQ may communicate to its staff and students, through its authorised managers, information which:
   - is relevant to the UQ as a whole (for messages to all, or large groups of staff or students) or to particular sections of the UQ such as Faculties, Schools or Divisions; and
   - is required for the effective functioning of the University or the relevant organisational unit; or which covers issues, policies, corporate events or decisions with a direct connection to the work of the University and its key organisational units.

h) Consumers must not send messages to a large number of recipients (e.g. all staff, all students, alumni, or a large volume of external users) without approval as outlined in the Information and Communication Technology Procedure.

i) Consumers may delegate mailbox access when required. If a consumer is unable to delegate mailbox access, authorisation must be provided by the Chief Information Officer.
2.6 Digital Presence

UQ’s digital presence includes websites, web applications, mobile applications and other means of providing information and services online. UQ’s digital presence must:

a) Comply with relevant legislation and UQ’s policies and procedures
b) Meet the needs of consumers
c) Be cohesive and consistent
d) Be accurate and up-to-date.

UQ will create and maintain its digital presence in accordance with the information provided in the Digital Presence procedure.

2.7 Information Management and Cyber Security

UQ seeks to respect the privacy and confidentiality of consumers and protect its information and assets. The following policies cover these matters:

- Information Management Policy
- Cyber Security Policy
- Privacy Policy

3.0 Roles, Responsibilities and Accountabilities

3.1 Consumers of UQ ICT Resources

Consumers are responsible for being aware of and complying with this policy. Consumers should also be aware that:

a) use of UQ ICT resources is subject to Australian laws and other relevant UQ policies. This includes but is not limited to copyright, breach of confidence, defamation, privacy, contempt of court, bullying and cyber-bullying, harassment, vilification, anti-discrimination, wilful damage and computer hacking; and
b) access to some third party applications and content has separate contractual arrangements and terms and conditions, which may apply over and above this policy.

It is the responsibility of consumers to check and maintain their UQ email account regularly.

3.2 Information Technology Staff

Information Technology staff are responsible for:

a) Provisioning ICT resources (e.g. consumer accounts, file storage, access to systems)
b) Monitoring the use of resources to determine violations of acceptable use
c) Technical enforcement of this policy including:
   a. preventing and monitoring access to inappropriate content.
   b. suspending consumer access when required and approved by CIO.
d) Complying with local standard operating procedures where applicable.

### 3.3 Chief Information Officer

The Chief Information Officer (CIO) is responsible for:

a) Ensuring that IT staff members are resourced to investigate alleged misuse.

b) Authorising the suspension of consumer accounts following investigations of misuse.

c) Ensuring this policy is maintained.

### 4.0 Monitoring, Review and Assurance

To improve services and protect consumers, UQ reserves the right to monitor ICT access and usage. Consumers should be aware that use of UQ ICT resources, including email, is not considered private, and that UQ may monitor, access, restrict, terminate or suspend accounts.

UQ will meet its data retention obligations under Schedule 1 of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth), recognising that UQ will rely on the ‘immediate circle’ exclusion for any relevant services provided only to persons who are ‘inherently connected to the functions of the University’.

### 5.0 Recording and Reporting

All usage (e.g. email, hard drives, or network use) may be recorded for the purposes of security and risk management (e.g. backups, performance monitoring, or compliance requirements).

Consumers who become aware of possible breaches of this policy must report it to either:

a) Information Technology Services

b) Their supervisor

c) The head of their Organisational Unit, or

d) The Chief Information Officer

Breaches of this policy may be reported to UQ’s Information Technology Governance Committee, the Chief Information Officer, the Chief Human Resources Officer, or to the appropriate external authorities which may result in civil or criminal proceedings.

### 6.0 Appendix

#### 6.1 Related Policies

a) Information Management Policy

b) Cyber Security Policy

c) Privacy Policy

#### 6.2 Related Legislation

a) *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth)
6.3 Definitions

Consumer - all staff, students, visitors, contractors, third parties, clinical and adjunct title holders, affiliates, alumni and all other people who access UQ's systems, networks or other ICT resources.

UQ ICT Resources – any UQ IT system or asset, including but not limited to:
- Networks (wireless and wired)
- Property and facilities
- Equipment whether owned or leased by UQ including Telephony, Computers, Servers, storage; including its Associated Hardware and software
- UQ websites and systems (applications)
- Data, information and video
- Accounts.

ITS – Information Technology Services
SITC – Strategic Information Technology Committee
ITGC – Information Technology Governance Committee

Unacceptable Material – includes materials not related to delivery of UQ’s core purpose or its effective operations, including but not limited to:
- Pornography
- Violent content
- Racist content
- Gambling or content relating to gambling
- Viruses and malware
- Games

Software - includes, but is not limited to, purchased or commercial software, sound, graphics, images, or datasets; shareware; freeware; and electronically stored documentation and the media that holds it. Not included in this definition are non-copyrighted computer data files that have no significance beyond the individual or organisational unit.

Software Licence Compliance - Clear documentation that the number of legally obtained and genuine software licences matches the number of installed instances of a given software product on the University’s systems or devices.

7.0 Meta Data for Document Management

<table>
<thead>
<tr>
<th>Web Links</th>
<th>Approval Authority</th>
<th>[Position]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Approval Date</td>
<td>[by group]</td>
<td>Notes</td>
</tr>
</tbody>
</table>

Ensure sufficient and correct metadata has been provided to enable effective document management.
1.0 Purpose and Scope

The University of Queensland (UQ) is committed to appropriately managing all forms of information that it creates and holds. Effective information management ensures that the right information is available to the right person, in the right format and medium, at the right time. Information that enables UQ to perform its core functions is considered an asset.

This policy outlines roles, responsibilities, expectations and requirements for managing information at UQ and is intended to enable UQ to:

- improve the integration and accuracy of its information,
- increase the impact of its research and scholarship,
- improve its compliance and reduce risks associated with potential loss or misuse of information,
- make better use of information in its decision-making processes,
- provide a strong foundation for systematically managing its information assets, ensuring that information of strategic importance is prioritised, and
- obtain valuable knowledge through the increased discoverability and accessibility of its information.

1.1 Scope

This policy applies to consumers of UQ information and communications technology (ICT) resources and anyone creating or accessing UQ’s information assets, including but not limited to:

- Students
- Staff
- Contractors and consultants
- Visitors
- Affiliates and third parties

Consumers that are connected to 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.

2.0 Principles and Key Requirements

Robust and effective information management at UQ:

- provides for the creation, use and sharing of information in compliance with legislative requirements and mandatory standards,
- helps to ensure that the right information is available to the right person, in the right form, at the right time, and
- is fundamental to UQ’s functions and operations.

The principles and requirements in this policy are related and intended to be applied by consumers as a whole where possible.
2.1 Information is treated as an asset

Information management supports evidence of UQ decisions and activities, enables accountability and transparency, mitigates risk, and allows businesses to operate. To achieve this, UQ ICT consumers must apply the following measures to their information management practices:

- Maintain adequate information and records (as outlined in the Information Management procedure) and capture this information in digital or physical management systems capable of meeting requirements of this policy and associated procedure.
- Follow the Information Security Classification procedure to classify all UQ information assets.
- Manage information throughout the information lifecycle (Create, Store, Use, Share, Archive, and Dispose) in accordance with the Information Management procedure. Information with historic, permanent or long-term value will be archived or preserved, and not destroyed.

Consumers should also seek to ensure digital information and records remain digital and will not be converted to a physical format unless required (the 'born digital, stay digital' principle).

UQ will maintain facilities to enable efficient cataloguing and discovery of information assets.

2.2 Information can be found and accessed

UQ facilitates the creation of large volumes of information. UQ consumers and members of the public should have access to certain UQ information where necessary. To achieve this:

- Non-confidential information about UQ will be available to the public.
- UQ will maintain procedures for responding to requests for information from the public.
- UQ staff will have timely access to information required to undertake their official duties, as authorised in the Information Management procedure.
- UQ staff will not give UQ records or information to unauthorised parties.

2.3 Information is suitable for all of its uses

The quality (completeness, consistency and accuracy) of information recorded must support UQ’s strategic objectives towards academic and research excellence. To achieve this, UQ ICT consumers should apply the following measures to their information management practices:

- Administrative records should be created as soon as possible after the event or action they document.
- The quality of information should be established at the point of collection in a suitable records management system. UQ will establish and maintain procedures for ensuring quality of information.
- Information recorded should consider the primary purpose for which it is collected or created and its potential secondary uses. High quality records management considers potential future secondary users of the information, which may not be known at the initial point of recording.

2.4 Information remains compliant

To strengthen its information and records management practices, UQ will:

- Comply with records and information management requirements in laws, regulations, contracts and agreements applicable to its operations (refer to section 6.2 and 6.3 of the appendix).
• Adhere to best practices and standards where possible.
• Establish and maintain records and information management guidelines and procedures.

Any records subject to legal processes (such as discovery and subpoena), required for internal or external review or investigation, or relevant to an application made under the Right to Information Act 2009 (QLD) must not be destroyed even if the retention period has passed.

This policy should be read in conjunction with other ICT policies and procedures and other UQ policies such as the Privacy Policy.

2.5 Information privacy, confidentiality and security is assured

To help protect UQ information and its consumers, UQ will:

• Safeguard personal and sensitive information and maintain controls for security of information as documented in the Cyber Security Policy.
• Establish and maintain procedures for the secure and appropriate sharing of confidential information.
• Preserve and maintain records to meet administrative, legal, fiscal and archival requirements and in accordance with at least the minimum requirements in relevant retention and disposal schedules.

3.0 Roles, Responsibilities and Accountabilities

Information management is the responsibility of all UQ stakeholders. Specifically, each information domain (e.g. Learning & Teaching, Research Management, or Human Resources) must have a designated Information Steward, one or more Information Custodians, and one or more Information Service Providers. The Steward and Custodian roles will usually relate to the organisational hierarchy associated with the business functions primarily responsible for managing the domain’s data. These roles are explained in more detail in the Information Ownership guideline.

3.1 Vice-Chancellor

The Vice-Chancellor must ensure UQ complies with the Public Records Act 2002 (QLD), including the principles and standards established by the Queensland State Archives. This responsibility may be delegated to relevant staff in accordance with the provisions set out below.

3.2 Chief Information Officer

The Chief Information Officer (CIO) is responsible for:

• Interpreting the business and information needs, and strategic goals of UQ and translating them into ICT initiatives that deliver value to UQ.
• Setting the strategic direction for UQ’s ICT and information management.
• Ensuring that Information Service Providers are adequately resourced to support this policy.
• Ensuring that alleged breaches of this policy are investigated.
• Ensuring that appropriate mitigation, reparation and punitive measures are taken following investigations of misuse (e.g. the suspension of consumer accounts).
• Ensuring this policy and supporting procedures are maintained.
3.3 Information Stewards

Information Stewards have authority over and accountability for the information in a domain and are responsible for:

- Reviewing and approving the standards, procedures, and other controls required for security, lifecycle management, risk management, and quality assurance of the information they steward.
- Ensuring that the management, use and protection of information is consistent with this policy, its associated guidelines and procedures, as well as relevant legislation, contracts and agreements.
- Assigning operational responsibility for information to one or more Information Custodians and ensuring resources are available to perform the required information management functions.

3.4 Information Custodians

Information Custodians ensure the rules for managing information in the domain are enforced on behalf of the Information Steward and are responsible for:

- Understanding, developing and recommending standards, procedures, and other controls for lifecycle management, risk management, quality assurance, appropriate use and security of information to the Information Steward and Information Service Providers.
- Implementing and maintaining the information security controls that enforce the rules and procedures for information and records management.
- Granting and revoking Information Consumers’ and Information Service Providers’ access to information and, when necessary, instructing them on the authorised uses of that information, as approved by the Information Steward.
- Enabling the timely detection, reporting, and analysis of security incidents where circumvention or attempted circumvention of controls takes place.
- Ensuring the information asset register is accurate for the domain.

3.5 Information Service Providers

Information Service Providers are responsible for:

- Delivering and supporting the systems, services, and information technology infrastructure required for UQ’s information management.
- Assisting Information Custodians to implement and maintain information security controls.
- Complying with information security controls in their own work, and reporting information security breaches to the appropriate Information Custodian as they arise.
- Performing system administration tasks including: physical site security; administration of security and authorisation systems; backup and recovery procedures; capacity planning; and system performance monitoring that ensure the reliability, integrity and functionality of business systems.
- Ensuring UQ information management is considered when decisions are made about systems.
3.6 Information consumers

UQ stakeholders accessing UQ information to undertake their roles are considered consumers and are responsible for:

• Complying with the rules and procedures approved by the relevant Information Steward for the use of information and records.

• Complying with controls implemented by Information Custodians and reporting information security breaches they become aware of to the appropriate Information Custodian as quickly as possible.

• Understanding and complying with UQ’s ICT policies and procedures.

• Relinquishing access to UQ information when it is no longer required to undertake their role.

3.7 Managers

UQ managers must ensure their staff are aware of UQ’s information management policies and procedures, and assign appropriate information management responsibilities to staff within their unit. Managers must also ensure documented information management systems are in place, consistent with UQ’s information management policies and procedures, to support business processes.

3.8 All staff

All UQ staff must ensure that records are created and managed adequately to document evidence of the business events and activities associated with their work functions. Staff must also:

• Dispose of records in accordance with authorised Retention and Disposal schedules.

• Maintain confidentiality of UQ records and the privacy of personal information.

• Secure records against unauthorised access and release of information.

• Ensure all UQ records in their possession at the time of cessation of employment are recorded effectively within the appropriate system or transferred to the custody of their supervisor.

4.0 Monitoring, Review and Assurance

UQ’s Information Technology Governance Committee will review all ICT policies and procedures on an annual basis and conduct appropriate consultation as required.

5.0 Recording and Reporting

UQ will meet its data retention obligations under the Telecommunications (Interception and Access) Act 1979 (Cth.), recognising that UQ will rely on the ‘immediate circle’ exclusion for any relevant services provided only to persons who are ‘inherently connected to the functions of the University’.

The CIO will ensure periodic monitoring of recordkeeping is conducted to determine how well it supports UQ’s business and strategic goals. Results of this monitoring will be reported to the IT Governance Committee.
6.0 Appendix

6.1 Definitions

**Information** – Includes, but is not limited to, physical (e.g. paper records) or digital files (e.g. email, voicemail, meeting minutes, video and audio recordings) in any format (e.g. PDF, .wav, .docx, or .jpeg).

**Information Asset** - A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.

**Information domain** – A broad category or theme under which University information can be identified and managed. UQ uses the Topics and Entities outlined in the CAUDIT Higher Education Data Reference Model, in the context of business capabilities and organisation structures, as a guide to determine appropriate information domains.

**Information Standards** - Define and promote best practice in the acquisition, development, management, support and use of information systems and technology infrastructure which support the business processes and service delivery of Queensland public authorities.

**Record** - Information in any format that has been generated or received by UQ in the course of its activities, and which must be retained by UQ as evidence of its actions and decisions.

**Retention and Disposal Schedules** - Defines the status, minimum retention periods and consequent disposal actions authorised for specific classes of records.

6.2 Related legislation

- *Public Records Act 2002 (Qld)*
- *Right to Information Act 2009 (Qld)*
- *Electronic Transactions Act 2001 (Qld)*
- *Telecommunications (Interception and Access) Act 1979 (Cth.)*

6.3 Other reference material

- Queensland Government Records Governance Policy
- Queensland State Archivist disposal schedules:
  - University Sector Retention and Disposal Schedule
  - General Retention and Disposal Schedule (GRDS)

7.0 Meta Data for Document Management

<table>
<thead>
<tr>
<th>Web Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Authority</td>
</tr>
<tr>
<td>--------------------</td>
</tr>
<tr>
<td>Last Approval Date</td>
</tr>
<tr>
<td>Next Review Date</td>
</tr>
<tr>
<td>Audience / Users</td>
</tr>
<tr>
<td>Notes</td>
</tr>
</tbody>
</table>
1.0 Purpose and Scope
Cyber security enables confidentiality, integrity and availability of information assets by providing protection against malicious and accidental threats. Cyber security threats take advantage of weaknesses in technology, people and processes to harm information assets. The University of Queensland (UQ) manages cyber security risk to safeguard its mission and protect the interests of the people whose personal information it holds.

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.

1.1 Scope
This policy is broad and applies to parties at UQ that hold or process UQ information, including:

- Students
- Staff
- Third parties (e.g. suppliers, contractors, consultants and partners)
- Visitors

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.

2.0 Principles and Key Requirements

2.1 Cyber Security Framework
UQ's cyber security framework supports the UQ Cyber Security Strategy, which seeks to mitigate risk and protect UQ's information assets against increasingly aggressive and sophisticated cyber threats whilst continually adapting to UQ's rapidly evolving needs. The framework comprises policies, procedures, local operating procedures, standards, guidelines and systems governing and facilitating cyber security management at UQ. The key platforms of the framework are information management, cyber security risk management and cyber security incident management, as explained below.

- The specification of cyber security controls is incorporated into relevant IT standards or as separate cyber security standards.
- 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.
- 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.
- The Exception Procedure is available for instances where the standard is not suitable, otherwise the standard must be followed.
- Standards will be updated as required to reflect changes in security controls.
2.2 Information Management

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.

2.3 Cyber Security Risk Management

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:

- Maintaining a register of key information assets.
- Establishing a framework for performing cyber security risk assessments aligned with UQ’s Enterprise Risk Assessment Framework.
- Incorporating cyber security risk identification and assessment into processes impacting the use and processing of UQ information.
- Maintaining a register of cyber security risks with related controls.
- Reviewing risks at regular intervals and as a result of significant security incidents, threats or changes to business requirements.
- Implementing and strengthening controls to reduce risk.
- Evaluating the effectiveness of controls.

2.4 Cyber Security Incident Management

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. The source of a cyber security incident may be accidental, malicious, or significant exposure to a known threat.

The UQ Cyber Security Incident Management 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.

Cyber security incidents should be reported immediately to IT support.

2.5 Cyber Security Vulnerability Testing

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.
2.6 Roles, Responsibilities and Accountabilities

2.6.1 Consumers, UQ Staff and Contractors
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.

UQ staff and contractors are responsible for:
- Participating in cyber security training where relevant to their work role
- Acting consistently and responsibly to protect the University’s information assets by:
  - Complying with procedures in place to protect information assets
  - Incorporating safe cyber security practices into their work
  - Reporting risks to IT support.

2.6.2 IT Management and Staff
IT managers manage relevant cyber security risks and are accountable for compliance with relevant cyber security standards.

IT staff are responsible for:
- Complying with relevant IT and cyber security standards and local operating procedures
- Assisting the CIO to identify and develop suitable cyber security frameworks, standards and local operating procedures
- Monitoring IT systems and services for potential cyber security risks and threats.

2.6.3 System Owner
All UQ systems will have an assigned System Owner accountable for system operation and the management of cyber security risks specific to that system.

2.6.4 Security Architect
The Security Architect is responsible for:
- Facilitating, monitoring and supporting cyber security risk management and compliance practices.
- Developing and maintaining cyber security strategy, policy, procedures, frameworks, local operating procedures and standards.
- Incorporating cyber security into IT frameworks, local operating procedures and standards.
- Overseeing the implementation and operation of UQ’s cyber security controls with broad impact.
- Providing cyber security risk management information, resources and training to consumers.

2.6.5 Chief Information Officer (CIO)
The CIO is responsible for:
- Promoting the importance of cyber security risk management to UQ leadership and staff delivering IT services.
- Providing adequate resourcing for the management of cyber security risk.
• Reporting on cyber security risk to UQ’s Senior Management Group and Senate.

2.6.6 Suppliers or Partners Processing University Information

Unless otherwise stated in a contract or agreement with UQ, suppliers or partners processing UQ information are responsible for:

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

2.7 Monitoring, Review and Assurance

2.7.1 Ongoing Review

The CIO will review this policy at least every three years to ensure it aligns with UQ’s cyber security strategy and industry best practice.

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.

Information Technology Services will drive compliance with the policy using:

• Ongoing cyber security awareness activities.
• Checks in key IT processes to ensure cyber security risk management activities are performed.
• Technical enforcement
• Regular reporting of self-assessments by organisational units on required cyber security controls implemented to protect information assets.
• Audits to assess compliance and effectiveness of technical controls.

2.7.2 Internal Audit

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

2.8 Recording and Reporting

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:

• Current risk level
• Control effectiveness
• Maturity of the University’s approach to cyber security against best practise frameworks
• Financial status
2.8.1 Mandatory Reporting of Private Data Breaches

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.

2.9 Appendix A – Related Policies and Procedures

- Cyber Security Incident Management Procedure
- Cyber Security Framework
- Information Management Policy
- Cyber Security Risk Management Framework
- Cyber Security Standard Exception Procedure

3.0 Meta Data for Document Management

<table>
<thead>
<tr>
<th>Web Links</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Authority</td>
<td>[Position]</td>
</tr>
<tr>
<td>Last Approval Date</td>
<td></td>
</tr>
<tr>
<td>Next Review Date</td>
<td></td>
</tr>
<tr>
<td>Audience / Users</td>
<td>[by group]</td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>