THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

UQ CYBER SECURITY STRATEGY

2017-2020

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

Office of the CIO

UQ Cyber Security Strategy 2017-2020

Office of the CIO

NAME:	UQ Cyber Security Strategy		
DATE:	21/07/2017	**RELEASE:0.2**	Final
AUTHOR:	Marc Blum		
OWNER:	Chief Information Officer		
CLIENT:	Strategic Information Technology Council		
VERSION:	V0.2		

Contents

Document Summary

Purpose

This document describes a strategy for managing cyber security risk at the University of Queensland (UQ).

Intended Audience

- University Senate
- University Senior Management Committee
- Strategic Information Technology Council (Previously Strategic Information Management Committee)
- Information Technology Governance Committee
- University wide IT Community

Reviewers

- ITS Senior Management Group
- ITS Managers
- Information Security Group members

Approvers

- Mr. Rob Moffatt, AM , Chief Information Officer

Revision History

Version	Date	Author	Changes
V 0.1	15/06/2017	Marc Blum	First Draft
V 0.2	4/07/2017	Marc Blum	Significant revision in response to feedback from Rob Moffatt. Reformatted to be consistent with governance team documents.

1. Context

The Cyber Security Strategy goes hand-in-hand with the Information Technology Strategy in support of UQ's mission of "knowledge leadership for a better world".

The Cyber Security Strategy is designed to address the following key challenges:

- The need to manage a complex range of ICT systems and offer a diverse range of services in an academic environment which values openness, flexibility and usability;
- The need to support a high rate of information technology innovation in service of a premium student experience and academic endeavours in an increasingly globally competitive environment;
- The need to support agile business and ICT services, providing simple but secure solutions;
- The need to manage large numbers of constantly emerging security vulnerabilities across multiple systems and platforms;
- The need to manage a broad spectrum of information security issues impacting systems, people and processes;
- An aggressive and constantly changing threat environment. Attackers that seek to exploit vulnerabilities to compromise systems, user credentials, steal intellectual property, undermine the integrity of student grades, qualifications or academic research; financial fraud or to otherwise harm the business and reputation of the University;
- Increasing resource-constraints and compliance obligations;
- The need to assess performance, provide assurance and improve decision making relating to cyber security risks through metrics, benchmarking and reporting.

2. Vision

Information services that are underpinned by a well-implemented end-to-end security program to deliver optimised risk management whilst enabling innovation and agility. Cyber security services that provide assurance and metrics to the University to permit sound, evidence-based decision-making to facilitate the University's mission. A security-oriented culture extending from ICT specialists to the entire UQ community, enabling effective consideration of cyber security concerns across academic, research, support and ICT domains.

3. Mission

To effectively mitigate risk and protect UQ's information assets against increasingly aggressive and sophisticated cyber threats whilst continually adapting to the rapidly evolving needs of the University.

4. Principles

- *Cyber Security is everyone's business*. As technical solutions for cyber security have improved, attackers have increasingly targeted users to gain unauthorised access to an organisation's sensitive data assets. In striving to find the easiest or fastest way to perform a task, users may also bypass an organisations security controls. Hence users, and the processes they use to perform their work, are a key aspect of cyber security. A holistic approach is required, taking into account environment, systems, people and processes.
- *Optimised management of cyber security risk*. An approach is needed that applies a dynamic mix of security controls to achieve the maximum benefit to UQ.

- *Balancing cyber security with usability*. Information security mechanisms should impose as little burden to users as possible to achieve the required level of protection.
- *Cyber security as enabling innovation*. Information security should be viewed as an enabler, allowing the University to benefit from the rapid development of information technology without exposing itself to unacceptable risk.
- *Cyber security must be adaptable and agile*. Cyber security must keep pace with change in many dimensions including the University's business; Information Technology; Security Technology and approach; and the evolving threat landscape.
- *Continuous improvement of cyber security management.* Regular review of the effectiveness of every element of the information security management programme together with learning from security incidents is necessary to create a mature and effective practice.
- *Cyber security solutions should be as simple as possible*. Cyber security controls should work in concert with each other and the underlying information systems and processes to achieve the greatest risk reduction for the least increase in complexity.
- *Building security from the ground up.* Cyber security needs to be addressed as a fundamental requirement in the design, development and selection of information systems and processes, and throughout their lifecycle.

5. Key Strategies and Objectives

Strategy 1
A risk-based approach will be used, driven by UQ's business requirements; aligning cyber security risk with business risk to facilitate appropriate ownership by UQ's governing individuals.
Objectives
• A register of UQ's information assets will be created and maintained to understand protection requirements from the perspective of the teaching, research and support elements of UQ. • A register of cyber security risks faced by UQ will be created and used as the basis for optimised investment in controls and reporting of cyber risk to UQ governing bodies. • Cyber security risks will be regularly reviewed to inform the development and evolution of security controls, providing ongoing resiliency to cyber threats.

Strategy 2
Cyber security governance informed by best-practise frameworks, and leveraging UQ and IT governance, will be used to ensure cyber security risk is addressed broadly and effectively across UQ.
Objectives
• The UQ ITC Security policy will be rewritten to provide a strong basis for cyber security governance. • An overarching framework for cyber security will be developed with associated standards and procedures. • A cyber security management programme will be established to implement regular activities required by the framework. • Relevant UQ procedures and standards will be reviewed and updated to ensure cyber security requirements are satisfied.

Strategy 3
Architectural methods will be used to achieve an effective, well-balanced blend of technical and procedural controls.
Objectives
• A cyber security architecture will be developed and implemented to provide cohesion between technical controls for greater overall effectiveness. • Security will be incorporated into architectural design processes as a fundamental concern.

Strategy 4
A culture conducive to cyber security will be fostered at UQ to strengthen other security initiatives.
Objectives
• A comprehensive security awareness programme will be implemented to increase knowledge and promote the importance of cyber security.

Strategy 5
Collaboration will be used to improve UQ's security capability while contributing to broader initiatives to reduce the impact of cyber threats.
Objectives
• Strong collaborative relationships will be developed with information security service providers and peers in other Universities to augment and strengthen internal information security capabilities and contribute to broader initiatives to improve Information Security.

Strategy 6
The information security service capabilities of AusCERT will be leveraged to provide exceptional operational security to UQ.

6. Alignment with UQ and IT Strategic Goals

Enhancing the student experience by:

- Providing a safe and secure digital environment for students;
- Enabling confident adoption of innovative teaching and learning technologies without exposing UQ to unacceptable information security risk;
- Protecting students from cyber-crime by increasing information security awareness.

Enabling the research and academic endeavour by:

- Protecting intellectual property and valuable research data from security breaches;
- Providing information, advice and tools to the UQ community to facilitate secure collaboration;
- Enabling researchers to meet the information security standards needed for grants and external collaborations;
- Pragmatically managing the information security risk inherent in cutting-edge research;
- Providing appropriate security architectures and controls to facilitate high-speed research networks.

Delivering services that the UQ community values, including:

- Handling information security incidents effectively and sensitively;
- Protecting individuals and UQ by raising information security awareness.

7. Success Measures

The following changes in security metrics will be used to track the success of cyber security initiatives:

- Reduced residual information security risk to UQ.
- Increased risk mitigation due to implemented security controls.
- Increased level of maturity against best practise frameworks.
- Reduction in the average resolution time for security incidents.
- Increased proportion of users that have completed security training and respond appropriately to malicious emails.
- Increased proportion of hosts where security OS and application patches are up-to-date.