JCU Cybersecurity Management Plan

Information and Communications Technology

Table of Contents

1 Introduction 3

1.1 Scope 3

2 Roles and Responsibilities 4

2.1 University Council 4
2.2 Vice Chancellor 4
2.3 Deputy Vice Chancellor Services and Resources 4
2.4 ICT Advisory Committee (ICTAC) 4
2.5 Accountable Officer (Director ICT) 4
2.6 Asset Owners 5
2.7 Authorised Users 5

3 Controls 6

3.1 Risk Management 6
3.2 Policies 6
3.3 Organisation of Cybersecurity 7
3.4 Personnel Security 7
3.5 Asset Management 8
3.6 Access Control 8
3.7 Cryptography 9
3.8 Physical and Environmental Security 9
3.9 Operational Security 10
3.10 Communications Security 11
3.11 Systems Acquisition, Development and Maintenance 11
3.12 Supplier Relationships 11
3.13 Cybersecurity Incident Management 12

4 Definitions 13

5 Appendices 15

5.1 Appendix 1 - References 15

1 Introduction

Keeping Information and Communication Technology (ICT) systems and information secure in the face of constant changes in hardware, software, threats, and regulations is a prominent challenge. To ensure the processes, practices and technology remain effective, organisations must implement robust Information Security measures.

Practical and effective measures should encourage efficiency, be compliant with relevant laws, regulations and University policies and procedures, and ultimately seek to practically minimise risk to Information Security.

James Cook University's (JCU or "the University") Cybersecurity Management Plan provides the practical implementation of the Cybersecurity Policy. The Cybersecurity Management Plan specifies the baseline Information Security Controls (including procedures and processes) for the University to effect Information Security. This approach allows the business the flexibility to adapt components of the Management Plan to accommodate specific business objectives and requirements.

A set of goals have been established to provide clear direction for the evaluation and establishment of Information Security for the University. The aim and goals of the University's Cybersecurity Management Plan are as follows:

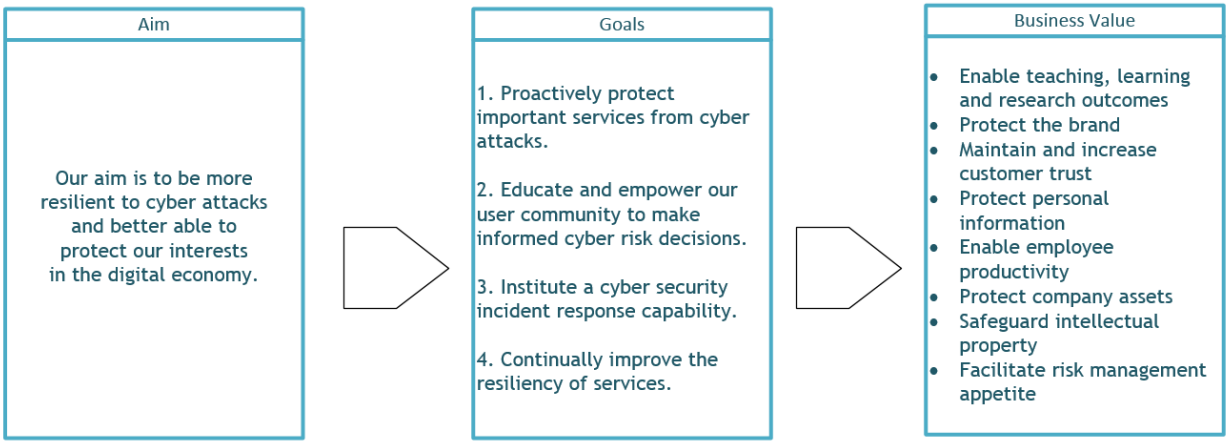

Figure 1 – JCU Cybersecurity Management Plan Aims and Goals

1.1 Scope

The Cybersecurity Management Plan applies to:

- University ICT Services.
- All Authorised Users of University ICT Services managed by the University or third party providers on behalf of the University, both on and off campus.
- Responsible Officers, the Accountable Officer and Asset Owners.
- The University's tangible and intangible assets including:
    - Reputation and public image; and
    - Information in any medium or form such as electronic (digital, video or audio representations) or printed paper.

The Cybersecurity Management Plan does not apply to:

- Controlled Entities of the University, including but not limited to:
    - JCU Singapore
    - JCU Health
    - JCU Vet
    - JCU Dentistry
- Third-parties.

2 Roles and Responsibilities

In addition to the responsibilities specified in the Controls, the following roles have responsibilities which apply to the Cybersecurity Management Plan.

2.1 University Council

The University Council is responsible for:

- Providing feedback to management on important Information Security matters/issues.

2.2 Vice Chancellor

The Vice Chancellor is responsible for:

- Supporting management in communicating the importance and benefits of Information Security risk management and awareness.

2.3 Deputy Vice Chancellor Services and Resources

The Deputy Vice Chancellor, Services and Resources is responsible for:

- Nominating the Accountable Officer;
- Sponsoring Information Security programs at an executive level;
- Maintaining oversight on the results of Information Security risk assessments and audits and reviews;
- Providing leadership on key Information Security matters; and
- Monitoring compliance with the Cybersecurity Policy.

2.4 ICT Advisory Committee (ICTAC)

The ICTAC is responsible for:

- Maintaining oversight of the effectiveness of the Cybersecurity Policy and associated strategies and plans;
- Ensuring appropriate roles and responsibilities have been defined;
- Overseeing the results of Information Security risk assessments, including residual risk;
- Overseeing the program of risk treatment implementation;
- Overseeing the continual improvement process (including audit findings); and
- Recommending resource allocation and financial support for Information Security programs and plans.

2.5 Accountable Officer

The Accountable Officer is responsible for:

- Setting the strategic direction for Information Security and establishing programs and plans including:
    - Awareness;
    - Risk Management; and
    - Response and Recovery.
- Establishing the University Cybersecurity Strategy.
- Establishing and articulating the University's attitude to Information Security risk (i.e. risk appetite criteria);
- Establishing a program of Information Security risk assessments for key business processes and systems;
- Ensuring the Cybersecurity Policy and Cybersecurity Management Plan remains aligned to the information and communication technology strategies of the University;
- Coordinating the day-to-day operation of the Cybersecurity Policy and Cybersecurity Management Plan;
- Managing resources and financial support for University Cybersecurity programs and plans;
- Establishing measurable objectives and reporting on these, at agreed intervals, to the Deputy Vice Chancellor, Services and Resources and ICTAC;
- Championing Cybersecurity programs and plans within the University as well as promoting the adoption of the Cybersecurity Policy throughout the University;
- Approving Cybersecurity audits and reviews;

- Providing Cybersecurity advice; and
- Reporting significant Information Security matters to management (including ICTAC, Audit and Risk Committee and University Council, as required).

2.6 Asset Owners

Asset Owners are responsible for:

- Including Information Security as a requirement in all new projects and initiatives, regardless of the type of project;
- Specifying, designing and implementing Information Security Controls to meet business needs and risk management objectives;
- Ensuring that appropriate Information Security Controls, consistent with the Cybersecurity Management Plan, are implemented;
- Monitoring for potential weaknesses and incidents; and
- Determining and reviewing access privileges.

2.7 Authorised Users

Authorised Users are responsible for:

- Actively engaging in awareness initiatives and programs;
- Complying with the requirements of Cybersecurity policies and procedures; and
- Reporting Information Security weaknesses or incidents in a timely manner.

3 Controls

3.1 Risk Management

Objective

To provide the management principles for effective Information Security within the University.

Scope

The Control applies to all University ICT Services.

Statement

The Accountable Officer will:

- Establish an enterprise Information Security risk management program in accordance with the principles of the University's Risk Management Policy and Framework. These include:
    - Assigning a Risk Owner (person or entity with the accountability and authority to manage the risk) to each Information Security risk;
    - Recording risk management decisions accurately; and
    - Reporting on Information Security risks through the appropriate committees.

  The Information Security risk management process will adopt an information centric risk governance model. This approach allows for:

    - Decisions to be made on the type of information risk;
    - Separate decision owners for each type of risk; and
    - Customisation of decision making processes for each event.

  The Information Security risk management program will be focussed on key business processes and systems. These will include (but not limited to):
    - Student management processes and systems;
    - Staff management processes and systems;
    - Financial management processes and systems;
    - Payment processes and systems;
    - Research processes and systems; and
    - ICT infrastructure processes and systems.

3.2 Policies

Objective

To provide the management principles for the effective Information Security within the University.

Scope

This Control applies to all University ICT Services.

Statement

The Accountable Officer will:

- Establish a set of Cybersecurity polices that are approved by management, published and communicated to stakeholders. These polices will include:
    - The Cybersecurity Policy; and
    - The ICT Acceptable Use Policy.

3.3 Organisation of Cybersecurity

Objective

To ensure that appropriate roles and responsibilities are in place to manage and protect University ICT Services.

Scope

This Control applies to all University ICT Services and Authorised Users.

Statement

The ICTAC will:

- Ensure that project submissions include responsibilities for the management of Information Security and risk.

The Asset Owners will:

- Establish appropriate segregation of duties within systems; and
- Include Cybersecurity requirements in all new projects and initiatives, regardless of the type of project.

The Director of ICT will:

- Maintain relationships with special interest groups to obtain advice on key vulnerabilities; and
- Disseminate vulnerability information to affected stakeholders on a timely basis.

3.4 Personnel Security

Objective

To ensure that personnel understand their Information Security responsibilities.

Scope

This Control applies to all Authorised Users.

Statement

The Director of Human Resources will:

- Partner with JCU management to ensure Cybersecurity clearance requirements are considered and assessed throughout the employment life cycle. This may include, but is not limited to, job design, recruitment and selection, internal transfer and off-boarding processes. Where potential risks are identified, measures will be undertaken to assess and then either accept, manage, mitigate or remove the risk as appropriate.
- Establish processes to notify relevant Asset Owners when the status of the University's staff changes. Asset Owners will ensure that all computer system privileges, building access privileges and other privileges have been disabled or removed as per the ICT Access and Account Management Procedures.

The Accountable Officer will:

- Ensure all Authorised Users receive appropriate Information Security awareness, education and training in organisation policies and procedures relevant to their role. This includes, but is not limited to:
    - Acceptable Use of University ICT Services; and
    - Security threats.

    Individual business areas may complement with additional training where necessary.

The Director of Student Services will:

- Establish processes to notify relevant Asset Owners when a student's status with the University changes.

The Asset Owners will:

- Ensure that all computer system privileges, building access privileges and other privileges have been disabled or removed, when notified to do so by Student Services or Human Resources.

The supervisors of Authorised Users (including Outside Users) will:

- Ensure all University owned assets are returned to the University upon termination of their employment, contract or agreement.

3.5 Asset Management

Objective

To define the requirements for asset classification and control. This includes both logical assets, for example intellectual property and information, and physical assets, for example equipment.

Scope

The Control applies to all University ICT Services.

Statement

The Director of ICT will:

- Establish a suitable information classification scheme for the University. The classification of information provides a level of criticality, sensitivity and protection standards. It also provides the basis for the level of controls needed to protect the information and/or system.
- Implement Controls for the Acceptable Use of University ICT Services.

The Asset Owners will:

- Ensure University ICT Services are designed and implemented in accordance with the information classification scheme requirements. Where technical requirements are not achievable, Asset Owners will implement Reasonably Practicable Controls based on the results of an Information Security risk assessment.

3.6 Access Control

Objective

To define Control requirements for access to University ICT Services.

Scope

This Control applies to all University ICT Services and Authorised Users.

Statement

The Director of ICT will:

- Implement the ICT Access and Account Management Procedures.

The Asset Owners will:

- Adopt a positive access enforcement model, whereby access to University ICT Services will be granted in a controlled manner driven by business requirements. Authorised Users do not have an implicit right of access to systems and resources, but instead access will be explicitly granted through the formal provisioning process;
- Provide Authorised Users with a unique identifier that enables accountability for the use of University ICT Services; and
- Ensure that unauthorised access to University ICT Services is prevented through the use of suitable authentication mechanisms, where core University ICT Services systems are not used for authentication.

3.7 Cryptography

Objective

To define proper and effective use of cryptography to ensure Information Security.

Scope

This Control applies to all University ICT Services.

Statement

The Asset Owners will:

- Implement and maintain cryptographic techniques to secure University ICT Services that transmit sensitive, confidential or personal information;
- Maintain cryptographic algorithms, key length and usage practices according to good practice; and
- Protect cryptographic keys from modification and loss.

3.8 Physical and Environmental Security

Objective

To define the physical and environmental security standards for Computer Facilities and ICT equipment.

Scope

This Control applies to all University ICT Services.

Statement

The Director of Estate will:

- Establish physical security measures to safeguard the physical security and integrity of University Computer Facilities. This includes:
    - Assessing new building designs for physical security risk and recommending appropriate controls;
    - Establishing a physical security perimeter and/or physical access methods for entry and exit based on the “need-to-know” principle of security;
    - Implementing and maintaining supporting utilities such as an uninterruptible power supply/generators for required assets;
    - Monitoring and recording (i.e. video) access to facilities to deter theft and maintaining stored recordings for a minimum of 14 days; and
    - Maintaining Estate plant and environment equipment.
- Establish processes for secure and sustainable disposal of ad-hoc ICT equipment.

The Director of ICT will:

- Implement or request implementation of supporting utilities (such as an uninterruptible power supply/generators) for ICT Data Centres; and
- Ensure secure and sustainable disposal of bulk managed ICT equipment, either directly or via second/third-parties.

3.9 Operational Security

Objective

To reduce the risk of errors occurring by the careful control of system operations.

Scope

This Control applies to all University ICT Services.

Statement

The Director of ICT will:

- Assess and implement supporting security measures to manage the risks introduced by using mobile devices;
- Routinely assess ICT managed systems and infrastructure for known vulnerabilities and provide the results to the responsible Asset Owner;
- Establish and implement appropriate Controls over University ICT Services including:
    - Change control;
    - Incident management;
    - Protection against malicious software, such as viruses;
    - Information back-up;
    - Event logging, monitoring and alerting; and
    - Patching and updating of systems.
- Ensure Disaster Recovery Plans for University ICT Services are established, maintained and tested to ensure systems and information are available, consistent with the University business and service level requirements.

The Asset Owners will:

- Establish processes to identify and respond to identified vulnerabilities.

3.10 Communications Security

Objective

To ensure the protection of information in networks.

Scope

This Control applies to all University ICT Services.

Statement

The Director of ICT will:

- Ensure that University managed networks are controlled and managed to protect users, information systems and applications. This includes:
    - Establishing responsibilities and procedures for the management of networking equipment;
    - Implementing controls to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks and to protect the connected systems and applications;
    - Implementing appropriate threat management, logging and monitoring to enable recording and detection of actions that may affect University managed networks;
    - Segmenting groups of information services, users and information systems on networks. Access between network domains is allowed, but should be controlled at the perimeter using an access gateway (e.g. firewall); and
    - Restricting access to sensitive network segments using two-factor authentication.

3.11 Systems Acquisition, Development and Maintenance

Objective

To ensure that information security is an integral part of information systems across the entire lifecycle.

Scope

This control applies to all University ICT Services.

Statement

The Asset Owners responsible for software development will:

- Establish principles for engineering secure systems. These principles will be documented, maintained and applied to any information system implementation efforts. The principles may include:
    - Security of the development environment and test data;
    - Coding guidelines for each programming language used;
    - Testing for security related vulnerabilities;
    - Security checkpoints within the project milestones; and
    - Ensuring control of source code repositories.

3.12 Third Party Contractual Relationships

Objective

To ensure protection of the organisation’s assets that are accessible by third parties.

Scope

This Control applies to all third party contractual relationships involving University ICT Services.

Statement

Asset Owners should:

- Use best endeavours to ensure that third party agreements appropriately address Information Security, privacy and confidentiality (particularly where the contractual relationship will involve access, transmission or storage of information (including personal and health information)).
- Seek advice from the University Legal Office where required to assist in compliance with this Control.

The Director of ICT will:

- Establish guidelines on the evaluation of third party Information Security controls (including cloud service providers).
- Ensure that ICT Projects identify and document risks relating to key technology / technology service suppliers (including cloud providers).

3.13 Information Security Incident Management

Objective

To ensure a consistent and effective approach to the management of Information Security incidents, including communication on security events and weaknesses.

Scope

This Control applies to all University ICT Services and Authorised Users.

Statement

The Authorised Users will:

- Report Information Security incidents through the appropriate management channels to relevant Asset Owners.

The Director of ICT will:

- Establish the University's Cybersecurity Incident Response Plan and ensure that responsibilities and procedures are established to ensure a quick, effective and orderly response to Information Security incidents, including supporting responses required by law (e.g. Notifiable Data Breaches).

4 Definitions

Term	Definition
Acceptable Use	Means those behaviours and actions, in connection with the use of University ICT Services, which are permitted under the ICT Acceptable Use Policy.
Accountable Officer	Means the senior staff member with accountability for Cybersecurity within the University, as appointed pursuant to the Cybersecurity Policy.
Asset Owner	Means an individual or collective group with accountability and authority for Information Assets.
Authorised User	Means a person who has been provided with an Authentication Credential by the University to access University ICT Services. Various categories of users are documented in the ICT Acceptable Use Procedures.
Computer Facilities	Means the buildings and rooms that contain University owned or controlled computer or ICT equipment.
Control	Means a measure put in place to manage, minimise or eliminate risk
Cybersecurity	Means the methods (policies, strategies, behaviours and techniques) through which necessary and commensurate measures can be identified, implemented, and maintained to effect Information Security.
Cybersecurity Control	Means a measure put in place to manage, minimise or eliminate Information Security risk.
Cybersecurity Strategy	Means a program of work that leverages industry standards and best practices to establish the necessary capabilities to achieve the University's Cybersecurity aim and goals.
Disaster Recovery Plans	Means those plans that specify the requirements for recovery of information systems and services in the event of a disaster, such as a flood, fire or major system failure.
Information Security	Means the protection and preservation of the confidentiality, integrity and availability of information in digital or other means.
Information Asset	Means an identifiable collection of data stored in any manner and recognised as having value for the purpose of enabling the University to perform its business functions, thereby satisfying a recognised University requirement.
Outside User	Means a person or organisation, external to the University.
Reasonably Practicable	Means that which is, or was at a particular time, reasonably able to be done to ensure Information Security, taking into account and weighing up all relevant matters including: • the likelihood of risk concerned occurring; • the consequence that might result from the threat or the risk; • what the person concerned knows, or ought reasonably to know, about the risk, and about the ways of eliminating or minimising the risk; • the availability and Suitability of Controls to eliminate or minimise the risk; and after assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.
Responsible Officer	Means a senior staff member or committee who makes, or participates in making, decisions that affect the whole, or a substantial part, of the business, namely the Vice Chancellor, Senior Deputy Vice Chancellor,

Term	Definition
	Deputy Vice Chancellors, Pro Vice Chancellors, Deans, Directors, Chief of Staff, Committees of Council and Committees of the Vice Chancellor.
Risk Owner	Means a person or entity with the accountability and authority to manage risk within the University.
Suitability of Control	Means the suitability of a particular Control having regard to whether or not the Control: • is effective in eliminating or minimising risk or the likelihood of risk; • does not introduce new and higher risks in the circumstances; and is practical to implement in the circumstances in which risk exists.
University ICT Services	Facilities and services provided to an Authorised User including software, communication devices, and computing infrastructure under the control of the University (or a third-party provider on JCU's behalf) that provides access to information in online or electronic format.
ICT Data Centres	Facilities, as approved by the Director of ICT, for the hosting of infrastructure to support University ICT Services.

5 Appendices

5.1 Appendix 1 - References

The following reference were used in the development of the Management Plan:

- JCU Cybersecurity Policy
- JCU Risk Management Policy
- JCU Risk Management Framework
- QLD Information Standard 18 - Information Security
- ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems - specification
- ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

Document Change Control

Version	Date	Authors	Summary of Changes
0.1	28/04/2016	ICT Security and Risk Specialist	Update following initial consultation and feedback from Tricia Brand, Raelene Eves and QPA.
0.13	5/05/2016	ICT Security and Risk Specialist	Update with Feedback from QPA. Submitted to ICTAC.
0.14	9/05/2016	ICT Security and Risk Specialist	Preparation for Legal Review
0.16	30/03/2017	ICT Security and Risk Specialist	Update to remove reference to a Framework Update following legal feedback from June 2016
0.17	3/07/2017	ICT Security and Risk Specialist	Update following legal feedback from July 2016
0.18	12/08/2017	ICT Security and Risk Specialist	Update following legal feedback from July 2016
1.0	13/07/2017	ICT Security and Risk Specialist	Final to approval

Administration

Approval Details

Guidelines	DVC Services and Resources
Version no.	18-1
Date for next review	13/04/2021

Revision History

Version	Approval date	Implementation date	Details	Author
18-1	13/04/2018	13/04/2018	Management Plan established	ICT

Keywords	Information, security, cybersecurity, risk, privacy, copyright,