JCU Cybersecurity Management Plan

Information and Communications Technology

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;

- 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.

3.3 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

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 suppo6(i)-24.1(c8(i)-24.1(p)24.2(l)x)-8(i)-242239 >>BDC /J 0.008 Tw -19.595

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

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

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.