Information Security Management Framework

Core Components

Purpose

This *Information Security Management Framework* (ISM Framework) aligns with and serves as an implementation strategy for the Information Security Policy (IS Policy).

The ISM Framework provides the conceptual structure for managing and supporting information security throughout the University and in compliance with JCU's operational requirements, relevant laws and regulations. Risk management is at the heart of this Framework, ensuring the identification, assessment, mitigation, and monitoring of information security risks in alignment with JCU's Risk Management Framework and Plan.

This Framework addresses HESF Standard 7.3.3(b).

Authority

In accordance with the IS Policy, the Accountable Officer delegated to lead and manage the ISM Framework is the Chief Information Security Officer. Revisions to this Framework will be managed and published to JCU's Policy Library.

Definitions

Refer to the Digital Infrastructure Policy Glossary for a comprehensive list of definitions, terms and explanations relating to information security at JCU.

Background and Context

JCU has well-established policies, procedures, and practices in place to protect the confidentiality, integrity and availability of its information management systems against security risks and threats.

These practices and processes are integral components of a comprehensive framework for managing all aspects of JCU's information security, including cybersecurity, and are collectively referred to as JCU's *Information Security Management System (ISMS).*

New and emerging initiatives will also continue to be reviewed, ensuring the identification of potential impacts on the ISM Framework. Integrating these into the Framework and its related processes will maintain its relevance and effectiveness.

Implementation Strategy

1. Integrated Implementation

In accordance with the IS Policy, JCU will integrate requirements from the following policy and standards into its practices and processes:

- Queensland Government Information Security Policy (IS 18:2018);
- ISO/IEC 27001 Information security, cybersecurity and privacy protection – Information security management systems – Requirements; and
- ISO/IEC 27002 Information security, cybersecurity and privacy protection – Information security controls.

In broad terms, these documents provide a suite of information security, cybersecurity and privacy protection controls and implementation guidance based on internationally recognised best practice. More specifically:

- IS 18 includes a *requirement* for JCU as a Statutory Authority, to implement an ISMS based on ISO 27001.
- ISO 27001 provides the *standards* for establishing, implementing, maintaining, and continually improving an ISMS.
- ISO 27002 gives *guidance* on implementing the standards contained within ISO 27001.

These are complex and comprehensive documents that include numerous security controls that can be used to measure and safeguard JCU's information systems, data, and assets from security risks and threats. **Table 1: ISO 27002 Overview,** includes the categories of these controls and the attributes used to group them.

Table 1: ISO 27002 Overview

Four Categories		93 Controls	Five Attributes
Organisational Controls	➔	37 Controls	Control Types
People Controls	➔	8 Controls	Information Security
Physical Controls	➔	14 Controls	Cybersecurity Concepts
Technology Controls	➔	34 Controls	Operational Capabilities
			Security Domain

To prioritise and streamline implementation of these controls, JCU will use the *National Institute of Standards and Technology (NIST) Cybersecurity Framework* (CSF) V2 to align the identified controls with JCU's existing practices and processes. This approach ensures a focussed implementation of the most critical security measures and the integration of internationally recognised standards with JCU's current security framework, thereby strengthening its overall security posture.

As the University continues to advance in its information management practices, it is committed to proactively adopting the broader scope of the IS and ISO requirements, in addition to other relevant frameworks and standards.

Table 2: ISM Maturity Assessment Process provides an overview of the implementation process. This process will guide the continuous assessment and improvement of JCU's information security management and maturity level.

Table 2: ISM Maturity Assessment Process

Step	Process	Description
1	Prioritise and Scope	• Identify JCU's business objectives and high-level organisational priorities to make strategic decisions regarding cybersecurity implementations and determine the scope of systems and assets that support the selected business line or process.
2	Orient	• Identify related systems and assets, regulatory requirements, and overall risk approach. • Consult sources to identify threats and vulnerabilities applicable to those systems and assets.
3	Create a Current Profile	• Develop a Current Maturity Profile for JCU.
4	Conduct a Risk Assessment	• Assess the operational environment to discern the likelihood of a cybersecurity event and the impact that the event could have on JCU. Identify emerging risks and use cyber threat information from internal and external sources.

Step	Process	Description
5	Create a Target Profile	- Create a Target Maturity Profile.
6	Determine, Analyse and Prioritise Gaps	- Compare the Current and Target Profiles to determine gaps and create a prioritised action plan.
7	Implement and Manage Action Plan	- Use the profiles to make informed decisions about cybersecurity activities, risk management, and cost-effective, targeted improvements.

2. Alignment of Security Controls to JCU's ISMS

As part of the implementation process, a comprehensive assessment and mapping will be conducted to align JCU's existing practices with IS 18, ISO 27001, and ISO 27002, and to identify opportunities for improvement. This is a continual process and subject to updates driven by JCU's business needs, privacy obligations and risk management processes. The mapping will be developed and maintained by the Manager, Governance, Risk and Compliance (Technology Solutions).

The mapping will follow the functions as established in NIST CSF, known as attributes in ISO 27002, and used to organise security activities at their highest level. These functions, as described below in **Table 3: NIST Functions**, are also applied to the planning process for Technology Solutions.

Table 3: NIST Functions

Function	Description
Govern	Develop and implement the organisation's cybersecurity risk management strategy, expectations, and policy.
Identify	Develop an organisational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities
Protect	Develop and implement appropriate safeguards to ensure delivery of critical services
Detect	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
Recover	Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Alongside this mapping process, resource allocation decisions, including time, personnel, and financial investments, will be made using a risk-based approach to address and mitigate threats and vulnerabilities.

3. Quality Assurance

3.1 Quality Framework

Information security at JCU will be governed by a broad set of documents relevant to individuals across various levels of the organisation. **Table 4: Document Overview** presents the distinctive characteristics of each document type and illustrates how they work collectively to ensure clarity, consistency, and adaptability within this context.

Table 4: Document Overview

Type	Description	Approved By	Located
Policies	- Establish high-level principles, objectives, and strategic directions for JCU, detailing the 'what' and 'why' aspects, including guiding principles and governance frameworks that must be adhered to across the organisation.	As per JCU's Governance Structure	JCU Policies and Procedures Library
Frameworks	- Define the structure for organising and integrating policies, procedures, and supporting documents, providing a comprehensive approach to managing specific domains (e.g., cybersecurity, risk management). Frameworks are treated with the same importance as policies within JCU.	As per JCU's Governance Structure	JCU Policies and Procedures Library
Procedures	- Detailed instructions for implementing policies and frameworks, specifying the 'how,' 'when,' and 'who' in the execution of tasks, ensuring compliance with organisational standards and requirements.	As per JCU's Governance Structure	JCU Policies and Procedures Library
Other Supporting Documents	- Ancillary documents such as guidelines, templates, forms, and handbooks that provide additional details, examples or instructions to support the application of policies, procedures, and frameworks.	As per JCU's Governance Structure	JCU Policies and Procedures Library (linked)
Other Related Documents and Resources			
Control Objectives	- Specific goals or conditions that articulate what needs to be achieved to meet the requirements of policies and frameworks, often aligned with risk management and compliance needs.	Chief Information Security Officer (CISO)	Technology Solutions Repository
Standards	- Definitive criteria or benchmarks that prescribe the expected level of quality, performance or compliance in processes, activities or controls, ensuring alignment with regulatory or organisational requirements.	Chief Information Security Officer (CISO)	Technology Solutions Repository
Standard Operating Procedures (SOPs)	- Detailed, step-by-step instructions designed to guide the execution of routine operations, ensuring uniformity, efficiency and compliance across all tasks.	Relevant Senior Manager	Technology Solutions Repository
Playbooks	- Prescriptive instructions or scenarios outlining the specific steps to be taken in response to particular events or situations, providing rapid and effective operational responses	Relevant Senior Manager	Technology Solutions Repository
Guidelines	- Recommendations or best practices aimed at guiding the interpretation and application of policies, frameworks, procedures and standards, allowing for flexibility while maintaining alignment with organisational goals.	Relevant Senior Manager	Technology Solutions Repository
Other Supporting Resources	- Other supporting resources such as the Website (e.g. Cyber Security Hub, IT Help Desk (ServiceNow), etc) facilitate and enhance operational functions.	Relevant Senior Manager	As appropriate

3.2 Compliance

A comprehensive and risk based internal assessment program will be implemented to evaluate the effectiveness of JCU's information security controls and measures. These assessments will align with NIST CSF, providing a structured process for evaluation.

The JCU Manager, Internal Audit will be consulted to facilitate a co-ordinated and effective approach, ensuring the preservation of the 3 Lines of Defence Assurance Model and allow for independent security system reviews to provide an increased level of confidence and trust.

The analysis of findings from all assessments and audits will be used to identify systemic issues and opportunities for improvement. Subsequently, the NIST Framework will be applied to assess JCU's security maturity and establish a roadmap for enhancing our cybersecurity posture.

4. Roles and Responsibilities

All policies and procedures will be developed and approved following JCU's governance framework.

4.1 The Chief Information Security Officer (CISO) is the Accountable Officer responsible for leading the implementation, management, and reporting of the Information Security:

- 4.1.1 Policy;
- 4.1.2 Management Framework;
- 4.1.3 Procedures; and
- 4.1.4 Control Objectives.

4.2 The relevant Senior Manager is the Accountable Officer responsible for leading the implementation, management and reporting of the Information Security:

- 4.2.1 Standards;
- 4.2.2 Playbooks, Process Flows, and other supporting documents and resources.

5. Management Review

In compliance with the Queensland Government Information Security Policy IS 18, JCU will conduct regular management reviews of its ISMS to ensure its continuing suitability, adequacy, and effectiveness. This requirement will be documented in a procedure encompassing the following considerations:

- Findings, actions and trends from:
  - Internal assessments and audits.
  - Non-conformances and corrective actions.
  - Feedback from stakeholders.
  - Results of risk assessments and risk treatment plans.
  - Opportunities for improvement.
- External and internal changes relevant to the ISMS.
- Changes in needs and expectations of relevant stakeholders.

Related policy instruments

Compliance Policy

Data Governance Policy

Digital Technologies Acceptable Use Policy

General Data Protection Regulation (GDPR) Procedure

Information Privacy Policy

Information Privacy Statement and Collection Notice

Information Security Policy

Cybersecurity Incident Response Plan

Personal Information Data Breach Procedure

Records Management Policy

Requests for Access and Amendment to Personal Information Procedure

Risk Management Policy

Risk Management Framework and Plan

Right to Information Policy

Staff Code of Conduct

Student Code of Conduct

Schedules/Appendices

Nil

Administration

NOTE: Printed copies of this policy are uncontrolled, and currency can only be assured at the time of printing.

Approval Details

Policy Domain	Corporate Governance
Policy Sub-domain	Risk, Assurance, Regulatory and Compliance
Policy Custodian	Vice Chancellor
Approval Authority	Council
Date for next Major Review	01/08/2029

Revision History

Version no.	Approval date	Approved by	Implementation date	Details	Author
24-2	01/10/2024	Vice Chancellor	01/10/2024	Minor amendments to Table 4: • Updates to all descriptions; • Removed *Process Flows* document type; • Added *Other Supporting Documents*, *Standard Operating Procedures* and *Guidelines* document types.	Information Security – Governance, Risk and Compliance Manager
24-1	01/08/2024	Council	07/08/2024	Major review – previously titled Cybersecurity Management Plan	Information Security – Governance, Risk and Compliance Manager

Keywords	Information security, cyber security, cybersecurity, NIST, ISO27001, ISO27002, IT
Contact person	Information Security – Governance, Risk and Compliance Manager