Information Technology and Security Policy

Section 1 - Purpose

(1) The purpose of this policy is to:

a. foster collaboration through shared accountability for information technology ('IT') investments, projects, risks, service decisions and performance
b. align funding, prioritisation of IT projects and resource allocation in line with the RMIT strategy and business objectives
c. encourage continuous service improvements of IT service performance
d. take measures to be resilient against information security incidents (including cyber-attacks) by maintaining adequate and effective information security capability
e. manage information technology risks and cybersecurity risks in line with the Risk Management Policy, and
f. comply with applicable state, federal and international laws governing IT assets.

Section 2 - Overview

(2) This policy acts as a base to support a mandated set of minimum security and technology standards that protect RMIT from technology-based threats to data, systems, personal information and health and safety.

(3) This policy outlines the information technology and security principles that underpin RMIT's approach to information technology management. It also details the responsibilities for senior officers as system owners and business owners, and for all users of RMIT information technology.

Section 3 - Scope

(4) This policy applies to all:

a. students, staff, contractors, visitors and any other parties who have access to the IT assets of RMIT University and its controlled entities ('RMIT')
b. IT assets owned, leased, operated, or under the custodial care of RMIT or third parties operated on behalf of RMIT.

Section 4 - Policy

Information Technology and Security Principles

(5) Alignment with RMIT Strategy - RMIT Information Technology Strategy aligns IT investment and initiatives with RMIT's strategic objectives and priorities.

(6) Optimise allocation of IT investments and resources – RMIT strategically allocates IT investments and resources across the enterprise.

(7) Maintain adequate and effective information security capability – RMIT ensures it has an adequate and effective information security capability that matches the nature of threats to its IT assets, allowing RMIT to operate smoothly.

(8) Implement security controls and undertake systematic testing – RMIT applies appropriate security controls prescribed in the NIST Framework 800-53 to safeguard its IT assets based on their security classification, and regularly tests these controls to ensure their effectiveness.

(9) Third party security and resilience capability - RMIT evaluates the information security and resilience capabilities of third parties that manage RMIT IT assets, based on the potential impact of a security incident and/or business continuity incident on those assets.

(10) Compliance with the Risk Management Policy – RMIT enforces accountability to manage technology and information security risks in line with the Risk Management Policy.

Information Technology and Security Governance

(11) RMIT publishes standards and procedures to implement principles in this policy.

(12) Infrastructure and Information Technology Committee ('IITC') considers, endorses, and monitors progress against the Information Technology strategy in accordance with RMIT Strategic Plan.

(13) Business Owners and System Owners are identified for all IT assets including the IT assets managed by third parties.

Responsibilities

(14) All users of RMIT information technology are responsible for:

a. ensuring that they understand and adhere to the standards, procedures and principles established by this policy in the context of their role
b. reporting and responding to incidents impacting systems, process, data, and cyber bullying or harassment as instructed
c. reporting all actual or suspected information security breaches immediately
d. engaging ITS for all procurement related to IT assets to ensure alignment with RMIT strategy, policies and standards.

(15) Business Owners are responsible for ensuring that:

a. ITS is engaged for all procurement related to IT assets
b. appropriate security classification levels, service classification levels and storage options are defined for IT assets under their ownership
c. where IT assets are managed by third parties, third parties have adequate security and resilience capabilities.

(16) System Owners are responsible for ensuring that:

a. compliance with the information technology standards and related resources published and communicated by Information Technology Services (ITS)
b. Business Owners are consulted to define appropriate security classification, service classification and storage options

c. relevant technology and information security risks are identified, analysed, assessed and actioned
d. relevant risk-based technology and security controls are identified, implemented and are operating effectively
e. third parties managing IT assets of RMIT have implemented adequate security and technology resilience controls relevant to the risks.

(17) The Chief Information Officer (CIO) is responsible for:

a. establishing and overseeing delivery of the Information Technology Strategy and Information Security Strategy
b. prioritising IT investments, initiatives, and resource allocation to optimise IT investments and resource allocation
c. overseeing delivery of Technology Strategy, Information Security Strategy, IT investments and initiatives
d. establishing and operationalising IT and security governance processes, technology operating model and policy framework to deliver reliable responsive and user-centric IT services
e. ensuring adequate and effective technology resilience capability including maintaining information security capability to ensure continued sound operation of RMIT
f. ensuring systematic controls testing program is set up to provide assurance on the design and operating effectiveness of the controls
g. ensuring that RMIT has robust mechanisms in place to detect and respond to information security incidents in a timely manner
h. ensuring that educational activities to raise awareness and educate users on how to reduce the risks of cyber security incidents have been delivered.

Compliance

(18) ITS monitors compliance with this policy and related obligations.

(19) Breaches of this policy will be managed in accordance with the RMIT Compliance Breach Management Procedure.

Review

(20) This policy will be reviewed every three years and undertake a major review every five years in line with the Policy Governance Framework.

Section 5 - Procedures and Resources

(21) This policy is to be read in conjunction with other RMIT policy documents which include but are not limited to the following:

a. Information Governance Policy
b. Privacy Policy.

(22) Refer to the following documents which are established in accordance with this policy:

a. Acceptable Use Standard - Information Technology
b. User Device Security Standard.

(23) The Chief Information Officer has delegated authority to create or amend resources enforceable under this policy.

Section 6 - Definitions

(Note: Commonly defined terms are in the RMIT Policy Glossary. Any defined terms below are specific to this policy).

Term	Definition
IT asset	Any information technology asset managed by RMIT or on behalf of RMIT. This includes software, hardware and the protection of information assets in digital format under custodianship of RMIT.
Technology resilience capability	Totality of resources, skills and controls which provide the ability and capacity to maintain technology resilience.
Information security capability	Totality of resources, skills and controls which provide the ability and capacity to maintain information security.
Business Owner	The individual responsible for the business functions that rely on the IT assets. The Business Owner ensures that the IT assets meet the needs of the business and are used in accordance with any relevant policies and regulations.
System Owner	The individual responsible for the overall ownership and management of a specific IT asset. They have the authority and accountability for the IT asset's operation, maintenance, and performance. The System Owner ensures that the system is designed, implemented, and operated according to the established ITS Policy, standards, and requirements.
Security classification	Data/information classification defined in line with the Information Governance Policy.
Service classification	Category of business service determined prior to the development of solution architecture in line with the Disaster Recovery Standard.

Status and Details

Status	Future
Effective Date	3rd June 2024
Review Date	3rd June 2029
Approval Authority	Senior Policy Advisor
Approval Date	18th April 2024
Expiry Date	Not Applicable
Policy Owner	Teresa Finlayson Chief Operating Officer
Policy Author	Sinan Erbay Chief Information Officer
Enquiries Contact	ITS Governance, Risk and Compliance