Information Technology and Security Policy

Section 1 - Purpose

(1) The purpose of this policy is to:

a. protect information resources against accidental or unauthorised disclosure, modification, or destruction and assure the confidentiality, integrity, and availability of University data and assets
b. apply appropriate physical, operational and technical safeguards without creating unjustified obstacles to the conduct of business and research of the university and the provision of services
c. comply with applicable state, federal and global laws governing information resources.

Section 2 - Overview

(2) Information technology and security principles underpin RMIT's approach to information technology management.

(3) This policy is the foundation for RMIT's information technology and security program and supports the University's Information Technology Strategy. It provides principles to support a mandated set of minimum security and operational standards that protect RMIT from technology-based threats to data, systems, personal information and health and safety.

Section 3 - Scope

(4) This policy applies to all:

a. RMIT students, researchers, staff, controlled entities of RMIT, contractors, visitors and any other parties who have access to RMIT's Information Technology Resources
b. information resources 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) RMIT information systems, tools and hardware are a shared resource for the benefit of RMIT authorised users only, to be used fairly, securely, lawfully and for legitimate University purposes.

(6) Access to RMIT Information will be available only to those with a legitimate need related to the business and operations of the University and its entities.

(7) Information generated by RMIT users relating to University business or operations remains the property of RMIT

and is accessible by authorised RMIT staff after termination of the account holder's employment.

(8) Information technology systems and solutions will be designed, sourced, implemented, and operated in ways that are secure, sustainable, cost effective and aligned to University strategy.

Responsibilities

(9) All users of RMIT information technology have a responsibility to:

a. adhere to standards and resources issued under this and related RMIT policies, including but not limited to, the Information Governance Policy and the Privacy Policy.
b. report and respond to incidents impacting systems process and data and/or cyber bullying or harassment as instructed. All actual or suspected information security breaches must be reported immediately.
c. keep their password secure, active and registered
d. ensure ITS endorsement is obtained for all software installed on the RMIT network,
e. keep data secure and apply data classification labels where available on RMIT systems.
f. engage ITS for all technology-related asset procurement, including IT hardware, software, and cloud services, to ensure alignment with RMIT strategy, policies, standards and the University's risk appetite

(10) All RMIT Information technology designers, implementors and operators have a responsibility to:

a. comply with information technology standards and related resources published and communicated by Information Technology Services (ITS)
b. implement logical, physical and environmental controls to secure information processing facilities and data
c. identify and comply with relevant global information security and privacy regulatory frameworks, relating to technology and data use, storage and transmission
d. design and implement controls that are proportionate to:
    i. information classification levels under the Information Governance Policy, and
    ii. the risk of unauthorised access, disclosure, modification, or destruction of information, whether accidental or malicious
e. follow governance requirements as directed by ITS including, but not limited to, Security Risk Assessment, Privacy Impact Assessment, ITS change and governance processes and standards, for all new technology solutions and services.

(11) Information Technology Services has a responsibility to ensure:

a. authorised users are informed and educated about their accountabilities, responsibilities and appropriate information technology practices
b. user activity is identifiable to an individual and may be monitored by duly authorised RMIT staff for security, compliance or other legitimate purposes
c. system logs, including audit, access, activity and performance logs are captured and retained according to regulatory and business needs
d. ICT services are measurable to the University's needs.

(12) The Chief Information Security Officer (CISO) has a responsibility to:

a. implement appropriate information security controls processes and technologies to protect RMIT and controlled entities from cyber security threats
b. maintain this policy and govern the publication of related information technology and security standards

c. implement capability for secure user access management for all RMIT authorised users
d. undertake risk-assessments of the technology control environment and advise on information security risks and controls
e. deliver educational activities to raise awareness and understanding of the obligations identified in this policy and educate users on how to reduce the risks of cyber security incidents.

Compliance

(13) Risk, Audit and Compliance is authorised to assess compliance with this policy and related obligations at any time.

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

(15) RMIT and third parties, must comply with all relevant global information security and related regulations and legislation.

(16) Third parties, including cloud services providing information technology or software services or resources, must have an information technology policy in place that provides no lesser security controls than RMIT's policy.

(17) Contractual arrangements with third parties must include security terms approved by the Office of the Chief Information Security Officer.

Review

(18) This policy will be reviewed at least once every three years in accordance with the Policy Governance Framework.

Section 5 - Procedures and Resources

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

a. Acceptable Use Standard - Information Technology
b. Information Security, Identity and Access Management Standard
c. User Device Security Standard

(20) Local ITS Cybersecurity Standards (resources) are available via the Cybersecurity Standards website. Resources enforceable under this policy may be amended or added to at any time with the endorsement of the Chief Information Officer.

Section 6 - Definitions

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

Information technology resources	Includes RMIT systems that hold RMIT information and ICT assets owned or licensed by RMIT, or on behalf of RMIT by a third party.
IT Business Partner	Role in ITS that works with university stakeholders to engage and deliver ICT services in the most effective way.
ICT asset	Any hardware or data used for or related to information technology or communication.

Status and Details

Status	Current
Effective Date	19th October 2020
Review Date	12th December 2022
Approval Authority	Vice-Chancellor's Executive
Approval Date	1st September 2020
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