Business Resilience Policy

Section 1 - Purpose

(1) The purpose of this policy is to:

a. maintain staff, student and visitor safety and wellbeing whilst ensuring RMIT's services to various stakeholders will continue to be available with minimal interruptions in the event of a critical incident, business disruption and/or IT disaster
b. establish RMIT's business resilience to enable RMIT to anticipate, withstand, respond and recover from potential threats, and the resultant impacts to business operations
c. safeguard people, processes, assets and place, in line with its dhumbali (commitment) to the Bundjil statement
d. manage business resilience risks in line with the Risk Management Policy, and
e. comply with relevant State, Federal and global laws.

Section 2 - Overview

(2) This policy outlines the principles, roles and responsibilities for RMIT's business resilience which encompasses the following three capabilities:

a. Critical Incident Management (CIM)
b. Business Continuity Management (BCM)
c. IT Disaster Recovery (ITDR).

Section 3 - Scope

(3) This policy applies to all employees, researchers, third parties and contractors of RMIT and its controlled entities.

Section 4 - Policy

Business Resilience Principles

(4) RMIT develops and maintains a comprehensive Critical Incident Management Plan, including clear protocols to ensure preparedness for a coordinated and strategic response to a range of potential critical incidents that may negatively impact RMIT.

(5) RMIT conducts systematic and periodic testing of the Critical Incident Management Plan using diverse scenarios to validate effectiveness in responding to real-world critical incidents, ensuring preparedness of the Critical Incident Management Team, identifying areas for improvement, and enhancing RMIT's resilience to a spectrum of potential situations or threats.

(6) RMIT establishes and maintains robust business continuity plans that cover people, processes, technology, sites,

facilities and third parties to enable essential staff to plan for and manage potential disruptions and for immediate and long-term consequences of incidents.

(7) RMIT conducts systematic and periodic testing of business continuity plans using diverse scenarios to validate their effectiveness in real-world disruptions to ensure preparedness, identify areas for improvement and enhance RMIT's resilience to a spectrum of potential threats.

(8) RMIT develops and maintains a thorough IT Disaster Recovery Plan that encompasses critical systems, data and infrastructure, outlining clear protocols for response, recovery and restoration to ensure minimal disruption to IT services during and after disaster in line with the Information Technology and Security Policy.

(9) RMIT implements a routine testing regimen for the IT Disaster Recovery Plan, conducting simulations and exercises to validate the effectiveness of recovery strategies, identify weaknesses and refine procedures to enhance RMIT's readiness to address diverse disaster scenarios.

(10) RMIT provides adequate training to prepare essential staff to manage critical incidents covering CIM, BCM and ITDR processes.

(11) RMIT ensures effective communication of information relating to incidents, disruptions, or disasters to all RMIT stakeholders. Incidents are managed and responded to in a coordinated, consistent, and sustainable manner.

(12) RMIT activates the three capabilities (CIM, BCM, IT DR) independently or in conjunction with each other depending on the nature and extent of the risk or threat, and all three capabilities are considered as part of key conversations, analysis, recommendations, and decision making.

(13) RMIT enforces accountability to manage business resilience risks in line with the Risk Management Policy.

Business Resilience Governance

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

(15) Business owners and system owners are identified for all CIM, BCM and ITDR plans including services managed by third parties.

(16) Audit and Risk Management Committee (ARMC) has regular oversight of business resilience capabilities and related critical incidents.

Responsibilities

(17) The University Executive Committee is responsible for monitoring the implementation of the policy and effective management of systems and processes that enables business resilience.

(18) The Executive Director Property Services is responsible for establishing Critical Incident Management capability, and the team is responsible for:

a. providing clear roles and responsibilities related to Critical Incident Management (CIM)
b. developing and maintaining effective and clear approaches, processes and plans for CIM
c. ensuring readiness of the Critical Incident Management Team (CIMT) to strategically manage critical incidents to protect RMIT's people, assets, business, financial and legal responsibilities, reputation, and regulatory requirements
d. supporting and collaborating with the ITDR team and BCM team to strategically manage disruptions, including communications, and protecting RMIT's brand and image in both testing and live incident scenarios, and executing plans accordingly

e. conducting Critical Incident Management training on an annual basis.

(19) The Chief Information Officer is responsible for establishing Business Continuity and IT Disaster Recovery capability, and the team is responsible for:

a. providing clear roles and responsibilities related to BCM and IT DR
b. developing and maintaining effective and clear approaches, processes and plans for BCM and IT DR
c. ensuring recovery objectives for IT systems are aligned with the business' expectations and are achievable
d. supporting the Critical Incident Management team during live disruption events and testing resulting in the invocation of business continuity plans and /or IT disaster recovery plans and/or Critical Incident Management Plan
e. conducting BCM and ITDR training and awareness on an annual basis across RMIT.

(20) Business owners are responsible for:

a. completing a Business Impact Analysis (BIA) in conjunction with the Business Continuity team to determine the effectiveness of Business Continuity Planning (BCP).
b. ensuring maintenance of overarching Business Resilience plans with up-to-date data and active participation in periodic tests along with essential staff.

(21) System owners must complete the disaster recovery planning and testing in conjunction with the Disaster Recovery team and in accordance with ITDR Standard.

(22) All employees, researchers, third parties and contractors are responsible for:

a. understanding and adhering to any responsibilities they may have under this policy including those from the underlying CIM, BCM and ITDR capabilities.
b. contributing to and participating in the identification, escalation and management of business resilience related risks or incidents

Compliance

(23) RMIT's Information Technology Services (ITS) and Property Services Group monitor compliance with this policy and related obligations.

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

Review

(25) This policy will undergo a major review at least every five years in line with the Policy Governance Policy.

Section 5 - Definitions

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

Business Resilience (BR)	is a strategy for anticipating disruptive events, ensuring rapid adaptation to potential incidents, maintaining uninterrupted business operations, and safeguarding people, assets, and the overall brand through three key capabilities: Business Continuity Management, Information Technology Disaster Recovery, and Critical Incident Management.

Business Resilience Plans	Business Resilience plans are Disaster recovery, Business continuity and Critical Incident management plans.
Critical incident or crisis	A Critical Incident is an abnormal and unstable situation that threatens an organisation or community and requires a strategic, adaptive and timely response in order to preserve its viability and integrity. (ISO 22361: 2022 Security and Resilience – Crisis Management – Guidelines).
Critical Incident Management (CIM)	An organisation's planned and coordinated activities to identify, lead, direct and control it's strategic response to a critical incident.
Incident and Major Incident (IT)	A situation that might be, or could lead to, a disruption, loss, emergency, or crisis. An IT Major Incident is defined as an unplanned or impending interruption or degradation of an ICT service with severe impact to the business of the University and its customers
Business continuity (BC)	The strategic and tactical capability of the organisation to plan for and respond to incidents in order to continue business operations at an acceptable pre-defined level.
Business continuity management (BCM)	A holistic management process that identifies potential threats to an organisation and the impacts to business operations if those threats materialise. BCM defines the foundations on which to build capability to effectively respond, to safeguard our stakeholders, people, technology, reputation, brand, premises and business processes.
Business impact analysis (BIA)	is a foundation step in business continuity management (BCM) to identify the organisation's critical business functions, supporting resources and people requirements, along with an identification of the negative impacts that would occur because of the inability to perform these functions over a period of time during an incident. The BIA enables the organisation to determine the business case, and the appropriate scope, for all continuity planning efforts.
IT Disaster Recovery (ITDR)	is the process of managing the continuity and recovery of critical technology infrastructure, systems, applications and digital services following a disruptive event.
Business Owner	The individual responsible for the business functions that rely on the people, process, technology, sites and third parties. The Business Owner ensures that RMIT 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.

Status and Details

Status	Current
Effective Date	2nd August 2024
Review Date	2nd August 2029
Approval Authority	Senior Policy Advisor
Approval Date	26th June 2024
Expiry Date	Not Applicable
Policy Owner	Fiona Notley Chief Operating Officer
Policy Author	Sinan Erbay Chief Information Officer
Enquiries Contact	ITS Governance, Risk and Compliance