MONASH University

Business Continuity Management Policy (BCM)

Purpose	The BCM model is designed to provide a systematic approach to the management of any adverse event that has the potential to damage Monash University and to establish basic principles for ensuring the recovery of time-sensitive or critical business operations that have been interrupted for any reason. The BCM model consists of policy, procedures and plans that provide the capability to continue the University's business operations with minimum impact in the event of an emergency, crisis or incident, to manage recovery, and identify opportunities for subsequent improvement.
A - Z Index of Terms	Please refer to "Definitions"
Scope	• The University community, facilities, equipment, IT infrastructure and systems, including every Australian campus or location. • Overarching principles apply to overseas campuses subject to local conditions and organizational structures • Certain types of emergency or crisis become the responsibility of external Emergency Services and crisis teams take directions accordingly.
Policy Statement	Monash University is committed to a Business Continuity Management (BCM) Framework that insures against strategic, operational, financial and stakeholder risks associated with service interruptions and critical incidents, specifically covered by four specialized areas: Crisis Management and Recovery, ICT Disaster Recovery, Incident Recovery and Emergency Response. The BCM Framework builds and enables a community of resources to: ▪ Ensure the welfare and safety of University personnel, students, contractors and visitors ▪ Protect the University's reputation and image ▪ Safeguard the continuity of teaching, research and commercial activity ▪ Ensure the integrity of the University's physical assets ▪ Enhance organizational resilience ▪ Identify and reduces risk exposures and potential economic losses ▪ Minimize legal liabilities ▪ Satisfy current regulatory requirements ▪ Make an appropriate environmental response ▪ Develop and continually improves BCM plans, procedures, and tools ▪ Protect the University's information, information systems and infrastructure.
Supporting Procedures	• Testing and Exercising for BCM • Crisis Management Procedures • ICT Security and Risk Framework (Draft) • Emergency Response Procedures

	• Incident Recovery Procedures
Supporting Guidelines	
Responsibility for implementation	▪ Chief Information Officer ▪ Executive Director Campus Community Division ▪ Security and Emergency Services Managers ▪ ICT Disaster Recovery Manager ▪ Business Continuity Analyst/IR Manager
Status	New
Key Stakeholders	▪ Vice-Chancellor's Group (VCG) ▪ Chief Information Officer ▪ Executive Director, Campus Community Division ▪ Executive Director, Buildings and Property ▪ Executive Director, Strategic Marketing and Communications ▪ Director – Risk and Compliance ▪ Director – Internal Audit ▪ Faculty Deans ▪ Other Divisional Heads where appropriate
Approval Body	**Name:** Mr Peter Marshall, Chief Operating Officer and Senior Vice-President. **Meeting:** TBA **Date:** 27-July-2017 **Agenda item:** TBA
Endorsement Body	**Name:** Vice-Chancellor Executive Committee (VCEC) **Meeting:** TBA **Date:** TBA **Agenda item:** TBA

Definitions	**BCM Community:** University staff members who are the responsible officers within the Incident Recovery, Crisis Management and Recovery, ICT Disaster Recovery and Emergency Response teams at operational or divisional level or who are engaged in or assigned to BCM activities as Team members. **Business Continuity Governance:** A stable framework providing leadership and clear lines of authority that can withstand changes to personnel and internal structures and facilitate better integration between a variety of incident responses. **Business Continuity Management (BCM):** A holistic management approach (including policies, standards and procedures) for ensuring critical business functions can be maintained or recovered promptly in the event of a disruption. **Business Impact Analysis:** The identification and prioritization of recovery

	priorities for specific faculties, divisions, schools, and teams. This includes critical business functions, recovery timeframes, resources, and dependencies **Crisis:** An adverse incident or series of incidents that have the potential to seriously damage Monash University's community, reputation, business operations, resources or property. **Crisis Management:** The strategic level management of crises through the use of a defined BCM methodology to develop, coordinate and implement a comprehensive plan for the University-wide response to a crisis. **Emergency:** A sudden, unexpected event that endangers or threatens the University's community or resources and requires an immediate response from internal or external agencies and emergency services. **ICT Disaster Recovery:** A comprehensive ICT strategy with a set of recovery plans to restore technological infrastructure to acceptable levels within a pre-determined period of time following an Incident. **Incident:** A range of scenarios including but not limited to: natural disaster (both onshore and overseas); power outage, data corruption, hardware/telecommunications failures; human activity, injury or death; explosives, chemical, biological and nuclear hazards. **Incident Recovery:** A management methodology that comprehensively plans for the response to a disruptive Incident, and the recovery of Critical Functions to Business as Usual (BAU) after an Incident in order to continue business operations at an acceptable predefined level **University Business:** Any activity conducted either in the course of employment as part of or related to a University course or other University functions **University Community:** Monash University staff and students, University Council members, contractors, consultants, visitors and clients of the University.
Related Legislation	Tertiary Education Quality and Standards Agency (TEQSA) Act 2011 Privacy and Data Protection Act 2014(Vic) Monash University Act(2009)(Vic) and subordinate legislation Occupational Health and Safety Act 2004 (Vic)
Related Policies	Bomb Threat Policy Civil Disturbance Policy Crisis Management Policy ICT Security & Risk Policy Security Incident Reporting Policy Risk Management Policy
Supporting Research and Analysis	▪ Business Continuity Management Internal Audit Report 2012 ▪ BCI Business Continuity 'Good Practice Guidelines' 2013 ▪ AS/NZS 5050:2010, Business Continuity Managing disruption related

	risk ▪ BS ISO 22301:2012, Business Continuity Management System ▪ BS ISO 22313:2012, Business Continuity Management Systems
Related Documents	BCM Framework website Crisis Management & Recovery Manual (revised 2015) Emergency Response Plan ICT Security and Risk Framework (includes Disaster Recovery) Incident Recovery Plans
Date Effective	January 2017
Review Date	27-July-2020
Policy Owner	Chief Information Officer
Policy Author	
Content Enquiries	BCM@monash.edu

University Policy Use Only:

Version Number:	**Contact:** adm-PolicyBank@monash.edu