Critical Incident and Business Continuity Management Policy

Section 1 - Key Information

Policy Type and Approval Body	Administrative – Vice-Chancellor
Accountable Executive – Policy	Chief Operating Officer
Responsible Manager – Policy	Deputy Director, Risk, Audit and Insurance
Review Date	8 November 2027

Section 2 - Purpose

(1) This Policy outlines La Trobe University's (University) commitment to effective management of Critical Incidents and the maintenance of services through business continuity processes.

Section 3 - Scope

(2) This Policy applies to:

a. all campuses of the University;
b. all staff, students, Council members, volunteers and contractors; and
c. all activities that are under the control or direction of the University, whether conducted on or off University property.

(3) This Policy should be read in conjunction with the Critical Incident Management Framework (CIM Framework). For detailed action plans and related resources, the Critical Incident Team should consult the Crisis Management Plan, which outlines specific procedural steps and provides necessary templates for implementation. These documents ensure a uniform approach in managing Critical Incidents and Business Continuity throughout the University.

(4) Disaster Recovery (DR) and Information Services (IS) Incident Response plans are managed by the Chief Information Officer under separate policy documents.

Section 4 - Key Decisions

Key Decisions	Role
Declare a Critical Incident and convene the Critical Incident Team.	Chief Operating Officer or nominee
Control the University's strategic response and provide executive decisions and strategic direction relating to Critical Incidents (Level 3), and managing related Business Continuity responses.	Critical Incident Team

Section 5 - Policy Statement

(5) This Policy is underpinned by the following guiding principles:

a. ensuring the safety and wellbeing of staff, students, contractors, volunteers, guests and the public;
b. using a risk-based approach consistent with the University's Risk Management Framework;
c. ensuring University assets are protected and preventing harm to the environment;
d. ensuring normal operations are maintained or resumed as soon as possible;
e. ensuring compliance with all laws and regulations;
f. effectively managing financial implications;
g. ensuring that internal and public confidence is preserved through a visible and professional response; and
h. undertaking action to prevent re-occurrence and improving future responses.

Section 6 - Procedures

Part A - Incident Classification

(6) The University uses a risk-based incident classification process in alignment with the Risk Assessment Matrix found within the University's Risk Management Framework. All incidents are classified as Minor (Level 1), Major (Level 2) or Critical (Level 3) to determine the appropriate level of response required to manage incidents effectively. Refer to the table below for further details.

Incident Classification	Description	Responsible
Minor Incident (Level 1)	A local event or issue that: • has no more than a minor consequence rating in any risk category and little or no potential to escalate; and • can be resolved satisfactorily through standard procedures and business as usual (BAU) resources.	Local management with the support of Emergency Service Operators, Campus Security and Subject Matter Experts (SMEs) as required.
Major Incident (Level 2)	An event or issue that: • has no more than a moderate consequence rating in any risk category but potential to escalate; • may not necessarily be resolved satisfactorily by standard procedures and BAU resources; and • may include a Business Continuity response.	Senior management with the support of Emergency Service Operators, Campus Security and SMEs as required.
Critical Incident (Level 3)	A situation with a major or catastrophic consequence rating in any risk category and will be an event or issue that: • has a long-term or profound effect; • cannot be controlled through standard procedures and BAU resources; • needs high levels of resourcing and support to manage, including involvement of the Critical Incident Team; and • may require a Business Continuity response.	Critical Incident Team with the support of Emergency Service Operators, Campus Security and SMEs as required.

Part B - Key Phases

(7) The University's Critical Incident management procedures are outlined in the CIM Framework which support

coordinated decision-making through three key phases:

a. Respond: the immediate priority is to identify the nature and severity of the incident and to stabilise incident volatility by ensuring the health and safety of individuals, protecting property and assets, and preventing further loss or harm. Depending on the nature of the incident, the initial response may be supported by Emergency Services Operators, Campus Security or IT Helpdesk with the support of local and senior management, as required. The CIM Framework provides further guidance on identifying, reporting and escalating incidents.
b. Manage: the Chief Operating Officer(or their nominee) is responsible for declaring a Critical Incident (Level 3) and convening the Critical Incident Team to coordinate University management of the event. The activities of the Critical Incident Team are flexible, ensuring readiness to manage a range of incident scenarios. The team's structure, roles and responsibilities are set out in the CIM Framework. In addition, the Crisis Management Plan outlines actionable steps for a coordinated team response and contains a comprehensive Communication Plan.
c. Recover: if a Business Disruption occurs, the University will activate the appropriate Business Continuity Plan(s) to maintain or recover the Critical Business Activities impacted to an acceptable level until business-as-usual procedures have been resumed. Other recovery plans including DR and IS Incident Response plans should be implemented as required to support IT service restoration.

Part C - Buisness Continuity Management

(8) The University is committed to building and improving organisational resilience, which enhances its capacity to respond to an unexpected Business Disruption and resume operations in an efficient and orderly manner.

(9) Business Continuity requirements will be informed by a Business Impact Analysis (BIA) of the activities undertaken by the relevant Divisions. A BIA is a systematic process to identify and analyse the business activities that must be restored as a priority during a Business Disruption. As part of this process, Divisions are required to determine the target and maximum timeframes to restore each Critical Business Activity.

(10) The information gathered through the BIA process will assist Divisions in developing appropriate Business Continuity strategies to maintain or recover the identified Critical Business Activities, within defined timeframes. These strategies and the resources required for implementation should be documented in the Business Continuity Plan (BCP) for the relevant Division.

(11) To assist Divisions, the University's BCP template includes examples of specific disruption scenarios, where Divisions are required to document the corresponding recovery strategies for:

a. loss of key staff;
b. loss of access to building or facilities;
c. loss of IT systems; and
d. loss of critical suppliers.

(12) Continuity of service provision must be adequately addressed for services, infrastructure or any resources provided by third parties through service level agreements or other contractual arrangements in accordance with the assessed level of risk.

(13) The Critical Incident Team will determine whether a BCP is to be activated in response to a Critical Incident (Level 3) that has a sustained impact on Critical Business Activities. The Critical Incident Team will maintain primary responsibility for ongoing monitoring and decision-making of the Critical Incident and is responsible for advising and updating stakeholders of Critical Incident response activity. The University's BCPs can be enacted individually or simultaneously and will be managed by the relevant Division Heads, under the direction of the Critical Incident Team.

(14) Disruptive incidents that do not require involvement from the Critical Incident Team (ie, Major Incident (Level 2)), are managed at a local level by the relevant Division through the implementation of their BCP. Consideration must be taken for any other business area that might be impacted.

(15) Each Division Head will store a copy of their respective BCP, and the Risk, Audit and Insurance Team will maintain copies of all BCPs.

(16) The University's BCP template (other than IS related plans) is developed and maintained by the Risk, Audit and Insurance Team.

Part D - Training and Testing

(17) Regular updates and testing, knowledge development and awareness programs are to be undertaken as required to ensure that key staff are familiar with this Policy, the CIM Framework and the BCPs.

Part E - Responsibilities

Key Responsibilities	Role
• Promote this Policy, the CIM Framework and any other procedures and documents relating to Critical Incident and Business Continuity management. • Ensure members of the Critical Incident Team are aware of their responsibilities by delivering appropriate training.	Health and Safety Committee
• Provide central coordination, monitoring and reporting of all University Business Continuity management initiatives. • Facilitate governance reporting to Corporate Governance, Risk, Internal Audit and Safety Committee (CGRIASC), as required.	Risk, Audit and Insurance Team
Development and ongoing review of the Business Impact Analysis and the Business Continuity Plans within the respective Divisions	Division Heads
Cyber Security Incident Response Plan, IS Business Continuity Plan and IT DR processes	Chief Information Officer

Section 7 - Definitions

(18) For the purpose of this Policy and Procedure:

a. Business Continuity: means the capability of the University to continue to deliver services at an acceptable level during a Business Disruption.
b. Business Continuity Plan (BCP): means the documented procedures that guide the University to respond, recover, resume and restore to a pre-defined level of operation following a Business Disruption.
c. Business Disruption: means an incident or event that interrupts the University's Critical Business Activities, and cannot be managed through standard procedures. Incidents include both physical and non-physical events such as loss of infrastructure, major utility outages, IT system breakdowns, pandemics and natural disasters.
d. Business Impact Analysis (BIA): means the process of identifying and analysing Critical Business Activities and the impact that a Business Disruption might have on them.
e. Critical Business Activity: means an activity identified through the Business Impact Analysis process which must be maintained or restored to an acceptable level within a defined timeframe in the event of a Business Disruption. These activities, if interrupted, could lead to a range of risks including financial, health, reputational and legal for the University.
f. Critical Incident: has the meaning given to that term in Section 5 (under 'Incident Classification').
g. Emergency Service Operator: means Fire, Police, Ambulance or any other external service providing emergency support in the event of an incident.

Section 8 - Authority and Associated Information

(19) This Policy is made under the La Trobe University Act 2009.

(20) Associated information includes:

a. Critical Incident Management Framework
b. Crisis Management Plan (under development)
c. Risk Management Framework
d. Emergency and Critical Incident Procedures

(21) This document aligns with the following standards:

a. Australian Standard 3745-2010 Planning for Emergencies in Facilities
b. NFPA 1660: Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs
c. AS/NZS 5050 (2020): Business Continuity – Managing Disruption-Related Risk
d. Australasian Inter-Service Incident Management System (AIIMS)

Status and Details

Status	Current
Effective Date	8th November 2024
Review Date	8th November 2027
Approval Authority	University Council
Approval Date	8th November 2024
Expiry Date	Not Applicable
Responsible Manager - Policy	Andres Hayem Deputy Director, Risk, Audit and Insurance
Enquiries Contact	Commercial, Legal and Risk

Glossary Terms and Definitions

"student" - Student is defined in the La Trobe University Act 2009 as: (a) a person enrolled at the University in a course leading to a degree or other award; or (b) a person who is designated as a student or is of a class of persons designated as students by the Council.

"staff" - Staff means any person employed by the University as per the definition in the La Trobe University Act 2009 (Vic).