

Critical Incident and Business Continuity Management Policy

Section 1 - Key Information

Policy Type and Approval Body	Governance - Council
Accountable Executive - Policy	Chief Operating Officer
Responsible Manager - Policy	Chief Commercial Officer
Review Date	2026

Section 2 - Purpose

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

(2) The Policy sets out the principles under which critical incident response and business continuity are developed and implemented to ensure that the University is equipped to respond to a variety of incidents or disruptions, to keep people safe, and to support the continuity of processes to achieve its business objectives.

(3) This Policy should be read in conjunction with the Critical Incident Management Framework and Crisis Management Plan which provides further guidance for the management of critical incidents, and the Business Continuity Management Framework which details the requirements of how business continuity is to be developed, implemented and managed for the University.

Section 3 - Scope

(4) 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.

(5) 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
Coordinating the Critical Incident Management (CIM) program across the University including ensuring elements of the Policy and CIM Framework are upheld.	Risk, Audit and Insurance (RAI) Team
Declare a critical incident and convene the Critical Incident Team	Chief Operating Officer (COO) or nominee
Coordinate the response to the critical incident	COO (or nominee) in their capacity as University Incident Controller
Ensuring members of the Critical Incident Team are aware of their responsibilities by delivering appropriate training.	Director, Facilities Assets and Services (or nominee) in their capacity as Operations Officer
Provide executive decisions and strategic direction on University priorities when responding to critical incidents and managing related business continuity responses	Critical Incident Team (CIT)
Custodians of Business Continuity Management(BCM) capability within their area and responsible for the development of Business Impact Analysis, which identifies systems required to ensure the business area continues to meet critical objectives during disruptions.	Divisional Heads
Coordinating the BCM program across the University including ensuring Business Continuity Plans (BCPs) are updated and tested in line with this Policy.	RAI Team
Cyber Security Incident Response Plan, IS Business Continuity Plan and IT DR processes	Chief Information Officer (CIO)

Section 5 - Policy Statement

(6) The University is committed to preventing, managing and recovering from critical incidents which disrupt core functions.

(7) In addition to the main principle of ensuring the safety and wellbeing of staff, students, contractors, guests and the public, the following principles underpin this Policy:

- a. Using a risk-based approach consistent with the University's Risk Appetite Statement;
- b. Ensuring assets are protected and preventing harm to the environment;
- c. Ensuring normal operations are maintained or resumed as quickly as possible;
- d. Ensuring legislative compliance;
- e. Effectively managing the financial implications;
- f. Ensuring that internal and public confidence is preserved through a visible and professional response; and
- g. Undertaking action to prevent re-occurrence and to improve future responses.

Section 6 - Procedures

Key phases

(8) Critical incident management supports coordinated decision making through three key phases:

- a. Respond: the immediate priority is to stabilise the situation by preserving life and property and preventing further loss. The initial response is supported by Emergency Services Operators in accordance with the University's Emergency and Critical Incident Procedures. In the event of an emergency, the immediate response is to dial 000 and request emergency services and then dial Campus Security on 03 9479 2222/ext. 2222.
- b. Manage: The COO (or nominee) is responsible for declaring a critical incident (Level 3) and convening the

Critical Incident Team to coordinate University management of the event as outlined in the Critical Incident Management Framework. The Critical Incident Team is responsible for the enterprise emergency management, internal and external communication, and enactment of business continuity activities.

- c. Recover: recovery activities commence with the University’s Business Continuity Plans which prioritise infrastructure, processes and resources which support core services. Recovery of University activities will build upon initial activities contained in the Business Continuity Plans until operations return to full function and capacity. Other recovery plans including DR and Cyber Security Incident Response plans should be utilised as required to support the restoration of service.

Classification

(9) Incidents are classified into three categories with key roles and responsibilities prescribed below. Full guidance of how these incidents are managed is found in the CIM Framework.

Incident Classification	Description	Responsible
Minor incident (Level 1)	An incident which results in low severity impacts including, but not limited to: <ul style="list-style-type: none"> • minor to moderate physical or psychological injury experienced by an individual; or • minor damage to a non-critical asset(s). A minor incident may be considered major where there is potential for it to escalate.	Local management with the support of Campus Security and Subject Matter Experts (SMEs) as required.
Major incident (Level 2)	An incident which results in moderate level impacts including, but not limited to: <ul style="list-style-type: none"> • significant physical or psychological injury experienced by an individual; • minor to moderate physical or psychological injury experienced by multiple individuals; • major damage to a non-critical asset(s); or • minor damage to a critical asset(s). 	Senior Management with the support of Emergency Service Operators, Campus Security and SMEs as required
Critical incident(Level 3)	An incident which results in significant level impacts including, but not limited to: <ul style="list-style-type: none"> • significant physical or psychological injury experienced by multiple individuals or a fatality; • major damage to a critical asset; • negative media attention by national media outlets leading to substantial reputational or financial impact; • regulatory breach leading to substantial reputational or financial impact (e.g. TEQSA, WorkSafe or OAIC); • major outage of critical technology; • inability of schools to teach or research; or • major cyber security breach. 	Critical Incident Team with the support of Emergency Service Operators, Campus Security and SMEs as required.

(10) The University is committed to the efficient and orderly resumption of critical business functions within acceptable timeframes. All BCPs should incorporate the identification of critical activities and associated recovery strategies covering the following key elements:

- a. Loss of People;
- b. Loss of Buildings;
- c. Loss of Systems; and
- d. Loss of Suppliers.

(11) BCP requirements will be informed by a Business Impact Analysis (BIA) of the activities undertaken by the relevant Divisions. A BIA is a systematic process that identifies and prioritises key activities of a business adversely affected by disruptions. Impacts will be assessed in accordance with the University's Risk Appetite Statement. Activities assessed as having the shortest recovery time objectives are deemed "critical activities". Recovery steps for these activities and their associated resources should then be documented in the BCPs.

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

(13) Full guidance on the required elements for an effective Business Continuity Plan are detailed in the Business Continuity Management Framework.

Plans and Testing

(14) 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 Critical Incident and Business Continuity Management Frameworks and the Business Continuity Plans.

- a. Critical Incident Management Framework including Crisis Management Plan
- b. Business Continuity Plans

(15) The following tests are to be conducted regularly:

Test	Owner
Local BC desktop tests are undertaken by each BCP area to roleplay their response to a high impact risk.	Divisional Heads
Critical Incident test which involves invocation of Critical Incident Team as well as the relevant BC teams to respond to an Enterprise level risk.	Critical Incident Team and Divisional Heads

Section 7 - Definitions

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

- a. Business Continuity Management (BCM): the capability of the University to continue delivery of services at acceptable predefined levels following a disruptive incident.
- b. Business Continuity Plan (BCP): the document to be referred to by the affected Divisional Business Unit during a disruptive incident, which outlines the steps required to restore critical services within recovery time objectives.
- c. Business Disruption: an interruption of normal business operations or processes which has the potential cause the services the University operates to fall below predefined levels.
- d. Business Impact Analysis (BIA): the process of analysing activities and the effect that a business disruption might have upon them.
- e. Crisis / Crisis Management: interchangeable terms with Critical Incident (see below).
- f. Critical Activities: a process or set of processes undertaken by the University that produces or supports one or more essential products or services.
- g. Critical Incident: an event that is likely to cause significant personal illness or injury, substantial impact on operations and commercial prospects, a degradation of reputation, or negatively impact the wider community.
- h. Critical Incident Management (CIM): a process which supports the University's coordinated response, management, and recovery from Critical Incidents.
- i. Critical Incident Team (CIT): the Critical Incident Management personnel comprised of the Incident Controller

and the personnel appointed to be responsible for the functions of planning, operations and logistics, which are listed in the Critical Incident Management Framework (Section 6).

- j. Emergency and Critical Incident Procedures: the protocols for responding to a range of critical incidents and emergencies, which are listed in the Critical Incident Management Framework (Section 5) and on the intranet.
- k. Emergency Service Operator: Fire, Police Ambulance or any other external service providing emergency support in the event of an incident.

Section 8 - Authority and Associated Information

(17) This Policy is made under the [La Trobe University Act 2009](#).

(18) Associated information includes:

- a. Critical Incident Framework
- b. Crisis Management Plan
- c. Emergency Response Procedures
- d. Business Continuity Framework
- e. Business Continuity Plans

Status and Details

Status	Not Yet Approved
Effective Date	To Be Advised
Review Date	To Be Advised
Approval Authority	
Approval Date	To Be Advised
Expiry Date	Not Applicable
Responsible Manager - Policy	Taryn Rulton Chief Commercial Officer
Author	Taryn Rulton
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).