

Name of Policy	Critical Incident Management Policy
Description of Policy	<p>This policy outlines ACU's commitment to effectively respond and manage Events, Incidents and Critical Incidents.</p> <p>Students, staff, contractors and visitors are required to comply with the Policy and all related Procedures including the Critical Incident Management Framework and Procedures.</p>
Policy applies to	<input checked="" type="checkbox"/> University-wide <input type="checkbox"/> Specific (<i>outline location, campus, organisational unit etc.</i>) <input type="checkbox"/> All Staff <input type="checkbox"/> All Students <input checked="" type="checkbox"/> Staff and Students
Policy Status	<input type="checkbox"/> New Policy <input checked="" type="checkbox"/> Revision of Existing Policy
Description of Revision	Revisions are to reflect the updated Critical Incident Management Program.
Approval Authority	Vice-Chancellor and President
Governing Authority	Chief Operating Officer & Deputy Vice-Chancellor
Responsible Officer	Deputy Chief Operating Officer
Approval Date	12 March 2018
Effective Date	12 March 2018
Date of Last Revision	25 November 2015 6 March 2018 11 February 2019 11 July 2019 9 August 2019 3 March 2020
Date of Next Policy Review (Unless otherwise indicated, this policy will still apply beyond the review date).	
Related Legislation, Policies, Procedures, Guidelines and Local Protocols	<ul style="list-style-type: none"> • Accident, Incident Reporting and Investigation Guidelines • Business Continuity Policy (currently in draft) • Business Continuity Framework (currently in draft) • Critical Incident Management Procedures • Email Distribution List Policy • Policy on Managing a Student Threatening Self-Harm (currently in draft) • Protection children and the vulnerable policy • Reportable Student Incident Management Manual • Reportable Student Incident Procedures • Reputational Management Plan • Risk Management Procedure • University Risk Register • Work Health and Safety Risk Management Program Guidelines

Table of Contents

1.0 Critical Incident Management Policy	3
1.1 Introduction	3
1.2 Purpose.....	3
1.3 Application	3
1.4 Scope.....	3
1.5 Accountabilities and Responsibilities	3
2.0 Critical Incident Management Categories	4
2.1 Events, Incidents and Critical Incidents Assessment Categories	4
2.2 Incident and Critical Incident Codes	6
3.0 Critical Incident Management Team	7
3.1 Incident Convenors	7
3.2 Incident Leads.....	7
3.3 Incident Response Group	7
3.4 Critical Incident Response Group	7
4.0 Critical Incident Management Process	8
4.1 Activation and Flowchart.....	8
4.2 Communication	8
4.3 Campus and Service Closure	9
5.0 Critical Incident Management Mitigation and Recovery	9
6.0 Appendices	10
6.1 Glossary and Terms.....	10
6.2 Flowchart	11

1.0 Critical Incident Management Policy

1.1 Introduction

Australian Catholic University engages with a large number of staff, students, contractors, volunteers and visitors. It operates and participates in a broad range of activities across Australia and overseas. The University recognises that an Event, Incident or Critical Incident may take place either on site at an ACU campus or facility, or off-site, and may happen at any time of the day or night.

The Critical Incident Management Policy encompasses the management of Events, Incidents and Critical Incidents from a human, hazard identification, and risk management perspective. It details the arrangements that apply to Critical Incident Management in the context of the University's Risk Management Framework.

1.2 Purpose

This Policy provides the guidance for ACU to plan for, respond to and manage Events, Incidents and Critical Incidents ensuring the University meets its duty of care obligations in providing the highest possible standard of health and safety and upholds its legislative obligations in relation to its staff, students, contractors, volunteers and visitors to ensure people are safe, and that ACU's reputation is maintained.

1.3 Application

This Policy applies to ACU and is subject to all applicable laws, regulations and codes.

This Policy and its related Procedures demonstrate ACU's commitment to:

- protecting the health and safety of staff, students, contractors, volunteers, visitors and the ACU community both in Australia and overseas;
- identifying and preventing Events, Incidents and Critical Incidents;
- allocating appropriate resources and building relationships to manage Events, Incidents and Critical Incidents in compliance with ACU's mission, legal obligations and standards;
- delivering the highest possible standard of health and safety for staff, students, contractors, volunteers, visitors, the ACU community and the public;
- managing its reputation for the benefit of students, staff, and stakeholders; and
- evaluating the effectiveness, adequacy and ongoing suitability of its Event, Incident and Critical Incident responses.

1.4 Scope

This Policy forms part of the Critical Incident Management Program which is the schedule of activities to ensure that the Critical Incident Management Policy, Procedures, roles and staff remain aligned. The Program falls within the overarching Critical Incident Management Framework.

This Policy applies to staff, students, contractors, volunteers and visitors while they are participating in University-related activities, both on and off campus, within Australia or overseas.

Nothing in this Policy overrides the Code of Conduct for All Staff Policy or Student Conduct and Discipline Policy.

1.5 Accountabilities and Responsibilities

The Deputy Chief Operating Officer, as the Responsible Officer for this Policy, is responsible for the establishment, operation, review and testing of the Critical Incident Management Policy and Procedures, including scheduling and coordinating scenario testing at least annually.

The Chief Operating Officer & Deputy Vice-Chancellor, as Governing Authority, will raise awareness of the Critical Incident Management Policy and Procedures to ensure that all staff, students, contractors, volunteers and visitors comply with their requirements.

The Deputy Vice-Chancellor (Education and Innovation) and the Director, Human Resources will also ensure students and staff receive information about this Policy and its related Procedures as part of their induction or orientation to the University.

Pre-defined members of the Incident Response Group and the Critical Incident Response Group will be trained for their roles and responsibilities within the Critical Incident Management Policy and Procedures. It is their responsibility to ensure staff within their business units are aware of their responsibilities to deliver the Policy and Procedures.

Staff who support the University’s business continuity and recovery processes are required to familiarise themselves with the Critical Incident Management Policy and Procedures.

2.0 Critical Incident Management Categories

2.1 Events, Incidents and Critical Incidents Assessment Categories

The following criteria apply to the categorisation of Events, Incidents and Critical Incidents.

Level		Criteria / Description	Responsible	Who to Notify
Level 0	Event	A minor issue that has a localised small impact on staff, students, contractors, visitors, volunteers, the ACU community and the public and may entail some property damage.	Local responsible staff (eg first aid officers)	Responses recorded as required in BAU processes and procedures
		<p>The Event has largely been contained and is unlikely to escalate in severity but still requires response and management by local ACU personnel. It can usually be handled using normal operating procedures.</p> <ul style="list-style-type: none"> Minimal impact on University Impact on small number of persons or property Event can be managed by responsible local staff or local campus facilities Emergency services may be notified Likely response will be less than 1 hour 	<p>Campus Facilities</p> <p>Emergency Services</p>	

Level		Criteria / Description	Responsible	Who to Notify
Level 1	Incident	<p>A moderate issue that has a localised impact on staff, students, contractors, visitors, volunteers, the ACU community and the public and may entail some property damage.</p> <p>The Incident has largely been contained and is unlikely to escalate in severity but still requires response and management by ACU personnel.</p> <p>It can usually be resolved using normal operating procedures.</p> <ul style="list-style-type: none"> • Emergency is affecting more than one building • Requires coordination of large volume of people • Coordination required to manage relocation from areas of campus • People have been injured, or there is potential of injury • Requires (multiple) emergency services • Requires management at off-campus locations • Requires management of key stakeholders • Media exposure at the local or state level • Likely response will be up to 4 hours 	<p>National Security Centre</p> <p>Incident Convenors</p>	<p>Incident Leads</p> <p>Incident Response Group</p> <p>Critical Incident Convenor</p> <p>External Regulators</p>
Level 2	Critical Incident	<p>A major issues or series of issues that have the potential to severely damage ACU's people, operations, environment, its long-term prospects and/or its reputation.</p> <p>It requires a significant response and on-going management.</p> <ul style="list-style-type: none"> • Large scale impact on University • Critical services impacted • Coordination required for complete campus evacuations or lockdowns • May impact staff, students, physical or virtual infrastructure or reputation • Requires management of key stakeholders and media • Requires strategic management • Media exposure at national or international level • Likely response will be more than 4 hours 	<p>Critical Incident Convenor</p>	<p>Vice-Chancellor and President</p> <p>Critical Incident Response Group</p>

2.2 Incident and Critical Incident Codes

Due to the broad definition of what comprises a Critical Incident, ACU is committed to applying the International Coding of Incidents to increase its response preparedness and effectiveness.

Colour Code	Type of Incident	Examples of Threats and Risks
Yellow	Internal Incident	<ul style="list-style-type: none"> ▪ Biological ▪ Chemical hazard ▪ Construction accident ▪ Critical equipment failure ▪ Gas leak ▪ Failure of essential services/utilities ▪ Industrial action ▪ Sabotage of building ▪ Structural damage ▪ Theft, fraud, malice ▪ Water damage
Silver	IT / Business Systems	<ul style="list-style-type: none"> ▪ Cyber Attack ▪ Data / records loss ▪ Business system failure ▪ IT equipment failure ▪ IT software failure
Red	Fire / Smoke	<ul style="list-style-type: none"> ▪ Fire ▪ Explosion ▪ Discovery of smoke/fire
Purple	Bomb threat	<ul style="list-style-type: none"> ▪ Bomb threat ▪ Suspicious item
Blue	Medical Emergency / Threat	<ul style="list-style-type: none"> ▪ EpiPen use ▪ Death staff / student ▪ Medical Emergency ▪ Poisoning ▪ Pandemic diseases ▪ Shock ▪ Asbestos exposure
Black	Personal Threat	<ul style="list-style-type: none"> ▪ Active Shooter ▪ Assault ▪ Child protection matter ▪ Robbery / Burglary ▪ Kidnapping ▪ Missing students / staff ▪ Self-harm, attempted ▪ Serious assault ▪ Siege ▪ Suicide ▪ Violent behaviour ▪ Terrorism ▪ Privacy
Green	Sexual assault/ harassment	<ul style="list-style-type: none"> ▪ Sexual assault ▪ Sexual harassment
Orange	Evacuation	<ul style="list-style-type: none"> ▪ Building evacuation
Brown	External	<ul style="list-style-type: none"> ▪ External party impact ▪ Natural disasters, earthquake, flooding, bushfire ▪ Off campus Incident ▪ Partner failure ▪ Public disorder ▪ Reputation ▪ Severe weather and storms ▪ Supplier Failure ▪ Third party negligence ▪ Transport accident

3.0 Critical Incident Management Team

3.1 Incident Convenors

Incidents will be allocated to one of the Incident Convenors based on these four categories - *Students, Staff, Physical, Virtual*.

Incident Convenors will manage the Incident and notify the relevant Incident Lead.

Incident Convenors and Categories	
Students	Director, Student Administration
Staff	Director, Human Resources
Physical	Director, Properties & Facilities
Virtual	Director, Information Technology
Critical Incident Convenor	Chief Operating Officer & Deputy Vice-Chancellor

3.2 Incident Leads

The Incident Lead works with the Incident Convenor and activates the Incident Response Group as required.

Incident Leads	
Ballarat	Campus Dean Ballarat
Canberra	Campus Dean Canberra
Strathfield	Campus Dean Strathfield
Brisbane	Associate Vice-Chancellor Brisbane
Melbourne	Associate Vice-Chancellor Melbourne
North Sydney	Associate Vice-Chancellor North Sydney
Rome	Provost and Deputy Vice-Chancellor (Academic)
Reputation	Director, Marketing and External Relations
Fraud	Chief Financial Officer
Privacy	Director of Governance
Sexual Assault / Harassment	Deputy Vice-Chancellor (Education & Innovation)
International	Pro Vice-Chancellor (Global and Education Pathways)
Student Accommodation	Director, Student Engagement and Services

3.3 Incident Response Group

The Incident Response Group can provide additional expertise and resources via local knowledge and skill to support the Incident Lead in managing an Incident, including recovery processes and access to required resources.

3.4 Critical Incident Response Group

The Chief Operating Officer is the Critical Incident Convenor and can declare a Critical Incident at their discretion and activate the Critical Incident Response Group (CIRG) if required.

The Critical Incident Response Group will include officers of the University who can provide their expertise, resources and support in managing a Critical Incident. The Critical Incident Response Group will oversee Critical Incident and recovery processes in conjunction with the Critical Incident Convenor.

4.0 Critical Incident Management Process

4.1 Activation and Flowchart

Event

When an Event occurs it is managed on campus by relevant campus resources or local emergency services. The Event is either resolved or escalated to an Incident and the National Security Centre (NSC) is notified.

Incident

Upon being notified of an Incident, the National Security Centre will notify the four Incident Convenors and the Critical Incident Convenor. The Incident will be allocated to one of the four Incident Convenors based on the category of *student, staff, physical, or virtual*.

The Incident Convenor triages the Incident and contacts the relevant Incident Lead to manage as required.

The Incident Lead manages the Incident and activates the Incident Response Group if required. The Incident is either resolved or escalated to a Critical Incident.

Critical Incident

The Critical Incident Convenor manages the Critical Incident and activates the Critical Incident Response Group if required. The Critical Incident Convenor notifies the Vice-Chancellor and Senior Executive Group.

See flowchart at Appendix 6.2.

4.2 Communication

All communication concerning an Incident or a Critical Incident will be coordinated by the Incident Lead (Reputation), who is the Director of Marketing and External Relations, in consultation with the Critical Incident Convenor

As per the ACU Email Distribution List Policy, staff designated as 'Convenor' or 'Critical Incident Convenor', their designated proxies and Executive Officers, and those additionally listed below, are authorised to send to all Dynamic DLs:

- Chief Operating Officer & Deputy Vice-Chancellor (Convenor)
- Deputy Chief Operating Officer (Proxy)
- Executive Assistant, Office of Chief Operating Officer

- Director Student Administration (Convenor)
- Associate Director, Student Systems (Proxy)
- Executive Officer, Office of Director, Student Administration

- Director Human Resources (Convenor)
- Associate Director, HR Business Partnering (Proxy)
- Executive Officer, Office of Director, Human Resources

- Director Properties and Facilities (Convenor)
- Associate Director, Facilities Management (Proxy)
- Executive Officer, Office of Director Properties and Facilities

- Director Information Technology (Convenor)
- Associate Director, IT End User Computing Services
- Executive Officer, Office of Director, Information Technology
- Director, Marketing & External Relations (Incident Lead Reputation)
- Associate Director, Communication and Creative Services (Incident Lead Reputation proxy)
- National Manager, Strategic Communications
- National Manager Strategic Projects, Office of Deputy Chief Operating Officer
- Program Officer, Office of Deputy Chief Operating Officer

4.3 Campus and Service Closure

In the event of an Incident or Critical Incident, ACU campuses remain open and staff are to stay at work until advice is received only from the Critical Incident Convenor.

The decision to close a campus is made when it is requested by State or Federal Government authorities, or decided by the Critical Incident Convenor to be necessary in the best interests of the campus students and staff.

5.0 Critical Incident Management Mitigation and Recovery

The University will identify strategies to facilitate the protection of people and assets and recovery of Critical Business Functions within agreed timeframes. This includes strategies to mitigate the impacts of an Incident or Critical Incident, including:

- protecting University property and infrastructure;
- stabilising the situation;
- continuing, resuming and recovering Critical Business Functions; and
- reducing the likelihood, length and impact of future disruptions.

Strategies will examine:

- response and recovery team structures and critical roles, including activation, escalation and communication procedures;
- Critical Incident Management Policy and Procedures;
- response action plans; and
- redundancy options for physical sites, operational infrastructure and technology.

5.1 Critical Incident Management Framework

The Critical Incident Management Framework will be regularly reviewed to ensure it:

- facilitates prompt action when adverse trends are detected or a non-conformity occurs; and
- continues to be an effective system for managing disruption-related risk.

Annual scenario exercises and recovery infrastructure testing will assist to:

- build familiarisation with staff roles, responsibilities, processes and available tools;
- identify practical program improvements; and
- provide a high level of stakeholder assurance in the University's recovery capability.

6.0 Appendices

6.1 Glossary and Terms

Term	Definition
Activation	The implementation of Critical Incident Management Procedures, activities and plans in response to a serious incident, emergency, or event.
Alternate Site	A pre-established site held in readiness for the recovery and resumption of business operations in the event of a disaster to maintain the organisation's mission critical activities and objectives.
Business area	A business area within an organisation e.g. department/ faculty.
Business Continuity	The strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.
Critical Incident	A Critical Incident is any emergency or adverse situation that will or may have the potential to significantly impact the university's business viability, threaten the lives of employees or others, and/or jeopardise the public image of the company.
Critical Incident Management	A holistic management process that identifies potential risks to an organisation and provides a framework for establishing resilience to ensure that the organisation is able to respond effectively to people injury, property damage or business disruption. This is achieved by formulating and implementing viable recovery strategies, developing a Critical Incident Management Plan and providing comprehensive training, testing and maintenance programmes.
Critical Incident Management Framework	The Critical Incident Management Framework is the overall approach, policies, and procedures to manage the University in the instance of Incidents and Critical Incidents
Critical Incident Management Program	The Critical Incident Management Program is the schedule of activities to ensure that the Critical Incident Management Policy, Procedures, Roles, and Assigned Staff remain aligned and ready to serve the University in the instance of Incidents and Critical Incidents.
Event	A localised, minor event that can be managed with local services and does not affect the ongoing viability of the organisation
Incident	A moderate event which interrupts business processes sufficiently to threaten the viability of the organisation.
Incident Response Group	A trained group of people responsible for operational management of an organisational-wide incident including response and recovery.
Response Strategy	A strategy to recover, resume and maintain all people safety measures, and infrastructure.
Risk	The effect of uncertainty on objectives.

6.2 Flowchart

