Name of Policy	Critical Incident Management Policy
Description of Policy	This policy outlines ACU's commitment to effectively respond and manage incidents and critical incidents. Students, staff, contractors and visitors are required to comply with the policy and all related procedures including the critical incident management procedures.
Policy applies to	☒ University-wide ☐ Specific (*outline location, campus, organisational unit etc.)*
	☐ All Staff ☐ All Students ☒ Staff and Students
Policy Status	☐ New Policy ☒ 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	Campus Board
Responsible Officer	Chief Operating Officer

Approval Date	12 March 2018
Effective Date	12 March 2018
Date of Last Revision	25 November 2015 6 March 2018
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	• Critical Incident Management Procedures • Reportable Student Incident Procedures • Risk Management Procedure • University Risk Register • Work Health and Safety Risk Management Program Guidelines • Accident, Incident Reporting and Investigation Guidelines • Reportable Student Incident Management Manual • Policy on Managing a Student Threatening Self-Harm (currently in draft) • Protection children and the vulnerable policy • Assoc. Vice-Chancellors and Campus Deans' Organisational Unit Risk Register • Reputational Management Plan • Business Continuity Policy (currently in draft) • Business Continuity Framework (currently in draft)

Table of Contents

1.0 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 incident or a 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 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 Policy 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 incidents and critical incidents;
- allocating appropriate resources and building relationships to manage incidents and critical incidents in compliance with ACU's mission, and 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, in the event of an incident or critical incident;
- managing its reputation for the benefit of students, staff, and stakeholders; and
- evaluating the effectiveness, adequacy and ongoing suitability of its incident and critical incident responses.

1.3 Purpose of this Critical Incident Management Policy

The policy provides the guidance for ACU to plan for, respond to and manage 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.

1.4 Critical Incident Management Policy

ACU's approach to Critical Incident Management incorporates the following key components:

- Development, implementation and annual review of Critical Incident Management Procedures, as outlined under Section 4 of this Policy.
- Testing the Procedures and supporting procedures.
- Training for staff with designated responsibilities during a simulated disruption, and for the development of general awareness for all staff.

1.5 Scope of this Critical Incident Management Policy

This policy applies to staff, students, contractors, volunteers and visitors – in the University workplace or while they are participating in University-related activities – on and off campus, locally within Australia and overseas.

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

This policy does not apply to the ACU Rome Campus, as this is a partnership with Catholic University of America, please refer the specific policy [The Rome Centre of The Catholic University of America (CUA) and the Australian Catholic University (ACU) Critical Incident Management Plan].

1.6 Exclusions

This policy does not apply to minor injuries or accidents that affect an individual or isolated area(s) and do not pose any additional threat or risk to staff, students, contractors, volunteers, visitors, property, or affect the University's operations and/or reputation. These minor incidents will be managed by activating ACU's WHS Accident and Incident Reporting, and Corrective Action processes.

1.7 Criterion for Activation of Critical Incident Management Procedures

The ACU National Security Centre (NSC) will immediately notify all primary Incident Response Group members when a situation is a potential Incident or Critical Incident.

The Incident Lead will activate the Incident Response Group (IRG), when an incident report is received from the ACU National Security Centre (NSC). The Incident Lead will select members of the Incident Response Group which includes officers of the University who will provide the right expertise to resolve the incident and apply learnings to reduce the risk of the incident from reoccurring.

1.8 Campus and Service Closure

In the situation where a Campus or Service Closure is required for safety, weather, utility failure or other adverse conditions (Codes Yellow or Brown), the Associate Vice-Chancellor, Campus Dean (Campus impact) or Services Director(National impact) may initiate a recommendation for the Campus or Service to close, if closure has not been directed by Emergency Services.

The Chief Operating Officer or Deputy Vice-Chancellor (SLT), following consultation with each other, the Associate Vice-Chancellor, Campus Dean (Campus impact) or Services Director (National impact), (or their delegate) can approve the closure of a Campus or Service.

2.0 Critical Incident Management Program Framework

2.1 Definition of Critical Incident Management

Incident

A moderate incident that has a localised impact on staff, students, contractors, visitors, volunteers, the ACU community and the public and may entail some property damage. The incident has largely been contained and is unlikely to escalate in severity but still requires

response and management by ACU personnel. It can usually be handled using normal operating procedures.

Critical Incident

A major incident or series of events that have the potential to severely damage ACU's people, operations, environment, its long-term prospects and/or its reputation. It requires a significant response and on-going management.

2.2 Incident Categories

Due to the broad definition of what comprises a critical incident, ACU is committed to applying the International Coding of Incidents to increase its preparedness and the effectiveness of ACU's response and management of incidents. The Incident Lead will manage an Incident, and initiate consultation with the Chief Operating, who will determine if the situation is to be escalated to a critical incident.

Colour Code	Type of incident	Threat/Risk	
Yellow	Internal incident	▪ Asbestos exposure ▪ Biological ▪ Chemical hazard ▪ Conflict of interest ▪ Construction accident ▪ Critical equip failure ▪ Cyber Attack ▪ Data / records loss ▪ Gas leak ▪ Failure of essential services/utilities	▪ IT equipment failure ▪ IT software failure ▪ Industrial action ▪ Plagiarism ▪ Power failure ▪ Sabotage of building ▪ Security access ▪ Staff resignation ▪ Structural damage ▪ Theft, fraud, malice ▪ Water damage
Red	Fire / Smoke	▪ Fire ▪ Explosion	▪ Discovery of smoke/fire
Purple	Bomb threat	▪ Bomb threat	▪ Suspicious item
Blue	Medical Emergency / Threat	▪ Epipen use ▪ Death staff / student ▪ Medical Emergency ▪ Poisoning	▪ Pandemic diseases ▪ Shock ▪ Suicide
Black	Personal Threat	▪ Active Shooter ▪ Assault ▪ Child protection matter ▪ Intrusion or hold-up ▪ Kidnapping ▪ Missing students / staff	▪ Self-harm, attempted ▪ Serious assault ▪ Siege ▪ Violent behaviour ▪ Terrorism
Green	Sexual assault/ harassment	▪ Sexual assault ▪ Sexual harassment	
Orange	Evacuation	▪ Building evacuation	
Brown	External	▪ 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

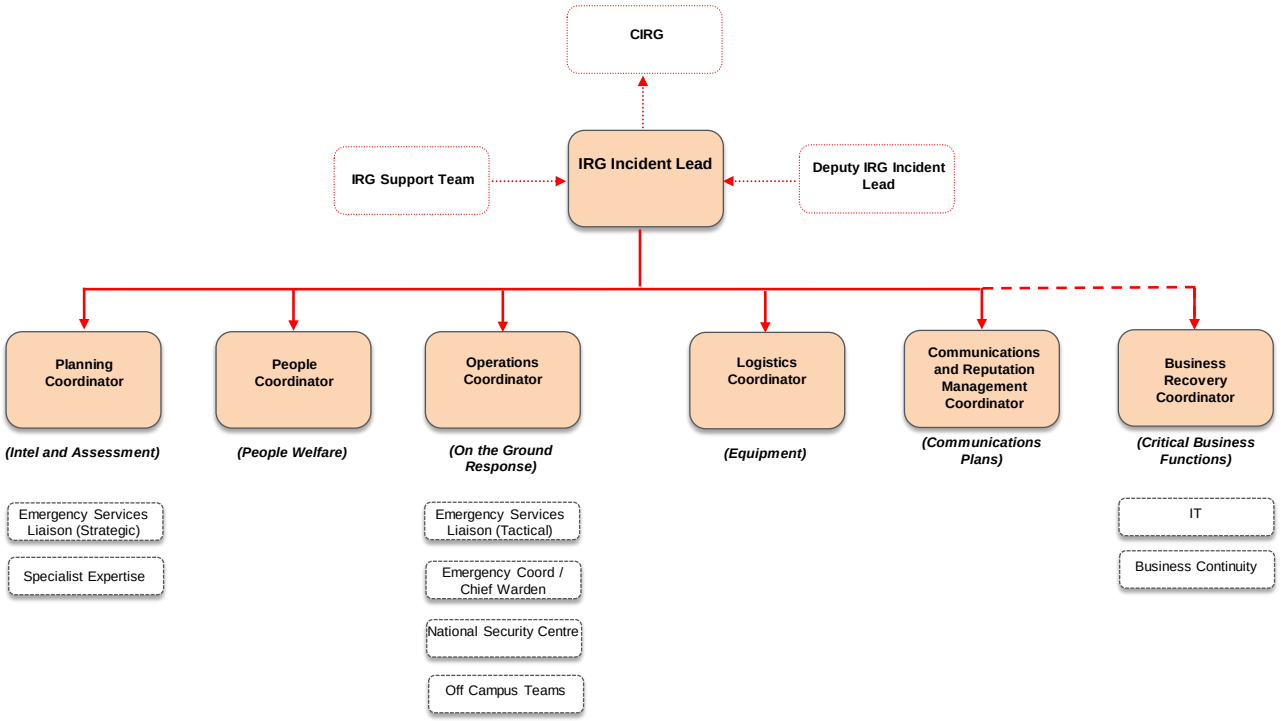
3.0 Critical Incident Management Team

3.1 Incident Response Group

Selection of staff and alternates on the Incident Response Group will be made by the Chief Operating Officer, with the key objective of membership being to include experienced staff from all major operational areas of ACU.

Depending on the location and nature of the incident, the following staff will assume the role of Incident Leads:

Incident Type / Location	Incident Lead
On Campus and/or satellite site incident (within Australia)	Relevant Associate Vice-Chancellor or Campus Dean by region
All Sexual Assault and Sexual Harrassment incident	Deputy Vice-Chancellor, Students, Learning & Teaching
Off Campus events/activities or student accommodation incident (within Australia)	Director, Student Engagement and Services
International incident	Pro-Vice-Chancellor, International
Rome Campus Incident	Provost &Deputy Vice-Chancellor (Academic)
Reputation Only incident (non-physical incidents)	Director, Marketing & External Relations
Information Technology Only incident (network, information security, software)	Director, Information Technology



3.2 Critical Incident Response Group

The Chief Operating Officer will declare a critical incident if it has the potential to significantly affect ACU's people, operations, environment or its long--term prospects and/or reputation.

The Chief Operating Officer will assume the role of Critical Incident Lead and activate the Critical Incident Response Group (CIRG) that will include officers of the University who can provide their expertise and additional resources and support to the Incident Response Group in managing the critical incident.

The CIRG will oversee Critical Incident and recovery processes in conjunction with the Incident Lead of the Incident Response Group.

3.3 Communication

All communication concerning an incident or a critical incident will be coordinated by the Director, Marketing and External Relations, in consultation with the Incident Lead and/or Critical Incident Lead.

3.4 Accountabilities and Responsibilities

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

The Chief Operating Officer will raise awareness about the Critical Incident Management Policy and Procedures. ACU is also committed to ensuring that all staff, students, contractors, volunteers and visitors – comply with the requirements of the policy and its related procedures.

Predefined members of the IRG and CIRG 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 related procedures.

The DVC, Students, Learning and Teaching; and the Director, Human Resources; will ensure students and staff receive information about this policy and its related procedures as part of their induction or orientation to the University.

Staff who support the business continuity and recovery processes are required to familiarise themselves with the policy and procedures.

3.5 Employment Arrangements

Should employees incur work related expenditure during an incident, or need to work overtime, these circumstances will be covered under the ACU Enterprise Agreement.

4.0 Implementation the Critical Incident Management Framework

4.1 Threat Identification and Mitigation strategies

Overview:

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 event, including:

- Protecting University property and infrastructure.
- Stabilising the situation.
- Continuing, resuming and recovering Critical Business Functions.

Strategies will examine:

- Response and recovery team structures and critical roles. This includes activation, escalation and communication procedures.

- Incident management procedures. This includes strategies relating to how an event is detected, assessed, monitored, recorded and communicated.
- Response action plans.
- Redundancy options for physical sites, operational infrastructure and technology.

Methodology:
Strategies will leverage off the response and recovery priorities based on the Threat Assessment process in 4.1. A process to mitigate risk will be applied when selecting strategy options. This includes:

1. Reducing the likelihood of a disruption.
2. Reducing the period of disruption.
3. Limiting the impact of disruption

4.2 Testing and Validation

The University Critical Incident Management Framework will be tested via a combination of scenario exercising and by periodic recovery infrastructure testing to confirm resumption of operational functions.

Testing and exercising will assist to:

1. Build familiarisation with staff roles, responsibilities, processes and available tools.
2. Identify practical program improvements.
3. Provide a high level of stakeholder assurance in the University's recovery capability.

The maximum interval between testing and exercising should be 12 months, unless there are valid reasons why the interval needs to be extended or material changes require a variation.

Upon the completion of the testing and evaluation, the Chief Operating Officer has delegated responsibility to make amendments to the Procedures.

5.0 Program Management

5.1 Review and Evaluations

The University will review and evaluate the performance of the Critical Incident Framework on a periodic basis. The objectives of the performance monitoring process are to:

- Facilitate prompt action when adverse trends are detected or a non-conformity occurs.
- Ensure that the University Critical Incident Management Framework continues to be an effective system for managing disruption-related risk.

5.2 Maintenance of the Program

The policy will be reviewed by Campus Board in consultation with – Planning, Quality and Risk Committee, Human Resources, Properties and Facilities Management, and Marketing and External Relations Directorates – on an ongoing basis to improve its effectiveness.

6.0 Appendices

6.1 Glossary and Terms

Term	Definition
Activation	The implementation of Critical Incident 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
Critical Incident Management Plan	A clearly defined and documented plan for use in the event of a business disruption. The plan provides a formal structure and guidance through checklists, strategies and other practical tools.
Disruption Event	An event that interrupts normal business functions, operations, or processes, whether anticipated (e.g, hurricane, political unrest) or unanticipated (e.g, blackout, terror attack, earthquake).
Incident	A physical event which interrupts business processes sufficiently to threaten the viability of the organisation.

Term	Definition
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.

ACU CRITICAL INCIDENT RESPONSE FLOWCHART