Critical Incident Management Policy

Section 1 - Purpose

(1) The Critical Incident Management Policy provides the guidance for ACU to plan for, respond to and manage Events, Incidents and Critical Incidents from a personnel, hazard identification, and risk management perspective.

(2) It ensures the University meets its legislative and duty of care obligations in providing the highest possible standard of health and safety to its staff, students, contractors, volunteers and visitors.

Section 2 - Scope / Application

(3) The terms “Event, Incident and Critical Incident” are used to define categories and levels of issues or disruptions and their associated response and management. For the purposes of this Policy, the term Critical Incident Management refers to all three levels (Event, Incident and Critical Incident) unless otherwise specified.

(4) The Critical Incident Management Policy and Critical Incident Management Procedure informs part of ACU’s Business Resilience Program.

(5) 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.

(6) Nothing in this Policy overrides the Code of Conduct for Staff or the Student Conduct Policy.

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

(8) This Policy and the Critical Incident Management Procedure demonstrate ACU’s commitment to:

a. identifying, managing and preventing Events, Incidents and Critical Incidents in compliance with ACU’s incident management procedures, the ACU Mission, Identity and Values, legal and reporting obligations and Risk Management Model and Principles;
b. evaluating the effectiveness and adequacy of its Critical Incident Management response and processes; and
c. managing its reputation by delivering the highest possible standard of health and safety for staff, students, contractors, volunteers, visitors, the ACU community and the public.

Section 3 - Roles and Responsibilities

Approval Authority

(9) The Vice-Chancellor and President is the Approval Authority for this Policy.

Governing Authority

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

Responsible Officer

(11) The Deputy Chief Operating Officer, as Responsible Officer, is responsible for the establishment, operation and review of the Critical Incident Management Policy and Procedure.

Other Relevant Stakeholders

(12) The Director, Student Experience, Director, Student Administration and the Chief People Officer will ensure students and staff receive information about this Policy and Procedure as part of their induction or orientation to the University. All staff who support the University's business continuity and recovery processes are required to familiarise themselves with the Critical Incident Management Policy and Procedure.

Section 4 - Categories and Codes

Events, Incidents and Critical Incidents Assessment Categories

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

Level	Type	Criteria / Description	Managed by
Level 1	Event	An Event is a localised, minor issue that can be managed with local services and does not affect the ongoing viability of the organisation. It is unlikely to escalate in severity but still requires response and management by local ACU personnel using appropriate processes and procedures. • Can impact staff, students, contractors, visitors, volunteers, the ACU community and the public. • Has minimal impact on University personnel or property. • May include minor personnel illness or wound. • Likely response less than 1 hour.	Local responsible frontline staff and supervisors
Level 2	Incident	An Incident is a moderate issue that can interrupt business processes sufficiently to threaten the viability of the organisation or the welfare of an individual or individuals. It could escalate unless it is responded to by ACU personnel using operating and incident response procedures. • Can impact staff, students, contractors, visitors, volunteers, the ACU community and the public. • Can result in people being injured, or there is potential of more severe injury (including threats of self-harm). • May require one or multiple emergency services. • Likely to affect one building or campus (but may be more). • May require coordination and evacuation of personnel. • Multiple IT / business systems may be affected. • May require management of key stakeholders. • Could escalate to involve media exposure at the local or state level. • Likely response up to or over 4 hours.	Incident Convenors Incident Response Group

Level	Type	Criteria / Description	Managed by
Level 3	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 jeopardise ACU's reputation. It requires a significant response and ongoing management including implementation of incident recovery processes and business continuity and recovery plans. • Large scale impact on University. • Critical services impacted. • May involve complete campus evacuations or lockdowns. • Requires strategic management of key stakeholders. • Likely to attract local, national or international media coverage. • Likely response more than 4 hours.	Critical Incident Convenor Critical Incident Response Group

Incident and Critical Incident Codes

(14) 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 or Critical Incident	Examples of Threats and Risks	
Yellow	Internal Incident	• Biological or 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	• Cyber attack • Data / records loss • Business system failure	• IT equipment failure • IT software failure
Red	Fire / Smoke	• Visible Smoke (not smoke alarm activation) • Fire	• Explosion
Purple	Bomb threat	• Bomb threat	• Suspicious item
Blue	Medical Emergency / Threat	• EpiPen use • Death staff / student • Medical Emergency • Poisoning	• Pandemic diseases / Pandemic with public or emergency orders • Shock • Asbestos exposure
Black	Personal Threat	• Active Shooter • Assault • Robbery / Burglary • Kidnapping • Missing students / staff	• Self-harm, attempted • Serious assault • Siege • Suicide • Violent behaviour • Terrorism • Privacy
Green	Sexual assault/ harassment	• Sexual assault • Sexual harassment	• Child protection matter • Privacy
Orange	Building evacuation	• Building Evacuation	
Brown	External	• External party impact • Natural disasters, earthquake, flooding, bushfire • Severe weather and storms	• Off-campus Incident • Partner failure • Public disorder • Reputation • Supplier Failure • Third party negligence • Transport accident

Section 5 - Responsible Staff

Incident Convenors

(15) Incidents are allocated to one of the Incident Convenors based on five categories - Students, Staff, Physical, Virtual, and Reputation.

Incident Convenors and Categories	
Students	Director, Student Administration
Staff	Chief People Officer
Physical	Director, Properties and Facilities
Virtual	Chief Information and Digital Officer
Reputation	Chief Marketing Officer
Critical Incident Convenor	Chief Operating Officer and Deputy Vice-Chancellor

(16) The Critical Incident Convener and each Incident Convener must nominate one proxy to act as Convener on their behalf.

Incident Response Group

(17) A new Incident Response Group is formed by the Incident Convener for the management of each Incident. Incident Conveners can select and approve any ACU staff for inclusion in an Incident Response Group. Staff are selected based on the Incident type, colour code and campus, to provide expertise and resources to support the Incident Convener during the management of an Incident.

(18) For the purposes of oversight and communication, the Critical Incident Convener and the five Incident Conveners are members of each Incident Response Group.

(19) Representatives from AskACU, Service Central and Facilities Management must be kept informed of decisions so that they can prepare for queries and provide a response that is consistent with the organisational message coordinated by the Incident Convenor (Reputation).

(20) The Critical Incident Management Procedure accompanying this Policy provides further guidance on organisational staff positions that may inform an Incident Response Group.

Critical Incident Convener and Response Group

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

(22) The Critical Incident Response Group includes the Incident Conveners and other officers of the University who can provide their expertise, resources and support to the Critical Incident Convener while managing a Critical Incident.

Section 6 - Activation and Management

Event

(23) Events (Level 1) are managed by local responsible frontline staff and supervisors including, but not limited to, staff from the National Security Centre, campus facilities, fire wardens, first aid officers, Student Administration,

Campus Ministry, Service Central, AskACU and Student Experience.

(24) The Event is either resolved or escalated to an Incident and the National Security Centre is notified.

Incident

(25) Incidents (Level 2) are managed by one of the five Incident Convenors (Students, Staff, Physical, Virtual, Reputation).

(26) The National Security Centre notifies the five Incident Convenors and the Critical Incident Convenor. The Incident is allocated to one of the five Incident Convenors who also determines the Incident Colour Code, campus location and Incident Response Group members.

(27) The Incident is either resolved or escalated to a Critical Incident.

(28) The Critical Incident Management Procedure that accompany this Policy provide further details on the incident management process and flowchart.

Critical Incident

(29) Critical Incidents (Level 3) are managed by the Critical Incident Convener in conjunction with the Incident Conveners and the Critical Incident Response Group.

(30) The Critical Incident Convener and Critical Incident Response Group provide regular updates on the management of, and response to, the Critical Incident to the Vice-Chancellor and President and members of the Vice-Chancellor's Advisory Committee, ACU staff and students, the Chancellor, members of Senate and external regulatory bodies, as required.

(31) ACU's Business Continuity and Business Impact Assessment information is utilised in the management of a Critical Incident.

(32) Refer also the Event, Incident and Critical Incident Response Flowchart for a visual representation of the incident management workflow.

Section 7 - Communication

(33) Incident Convenors should communicate regularly with their Incident Response Group and hold work-in-progress or briefing meetings during the management of an incident. During these meetings, communications to external or other stakeholders should be discussed and managed.

(34) All communication to staff, students, contractors, volunteers or visitors concerning an Incident or a Critical Incident will be coordinated by the Incident Convenor (Reputation), who is the Chief Marketing Officer, in consultation with the Critical Incident Convenor. AskACU, Service Central and Facilities Management are informed so that they can prepare for queries and provide a response to staff and students that is consistent with the organisational message coordinated by the Incident Convenor (Reputation).

(35) Such communication should be sent first and foremost by the Critical Incident Convener, however, staff designated as 'Convenor' or 'Critical Incident Convenor', their designated proxies and Executive Officers, and those additionally listed below, are authorised within the ACU Distribution List Policy to send to all Dynamic Distribution Lists for the purposes of communication information regarding a major university disruption.

- Chief Operating Officer and Deputy Vice-Chancellor (Convenor)
- Deputy Chief Operating Officer (Proxy)

- Executive Officer, Chief Operating Officer
- Director, Student Administration (Convenor)
- Associate Director, Student Systems (Proxy)
- Executive Officer, Office of Director, Student Administration
- Chief People Officer (Convenor)
- Associate Director, HR Business Partnering & Talent Management (Proxy)
- Executive Officer, People and Capability
- Director, Properties and Facilities (Convenor)
- Associate Director, Facilities Management (Proxy)
- Executive Officer, Office of Director, Properties and Facilities
- Chief Information and Digital Officer (Convenor)
- Associate Director, Client Services
- Executive Officer, Office of Chief Information and Digital Officer
- Chief Marketing Officer (Convenor)
- Associate Director, Communication and Creative Services (Proxy)
- National Manager, Strategic Communications
- National Manager, Strategic Programs, Office of the Deputy Chief Operating Officer
- Program Officer, Office of the Deputy Chief Operating Officer

Section 8 - Campus and Service Closure

(36) 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.

(37) 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.

Section 9 - Privacy

(38) Incident Conveners should consult the Privacy Officer to ensure that any disclosure of personal information associated with an Incident or Critical Incident is managed in accordance with the Privacy Policy, Privacy Inquiry and Complaints Procedure and Third Party Access to Personal Information Protocol.

Section 10 - Post Incident Report

(39) A Post-Incident Report should be delivered to Incident Conveners and the Critical Incident Convener within one week of the close of an Incident and a debrief meeting held within one week of the Post-Incident Report being received.

(40) A Post-Incident Report template is available in the Critical Incident Management Procedure that accompanies this Policy. The Report should be completed by the Convener who managed the Incident (or a designated member of their Response Team) and should:

a. assess:
    i. ‘What happened?’;
    ii. ‘What went well?’; and

iii. ‘What can we do differently?’.

b. be timely, accurate, interactive, objective and constructive, but not personal;
c. consider areas such as:
    i. Crisis Management – Plans, Structure, Notification, Escalation and Incident Assessment;
    ii. Communications – Systems, Internal, External, Timeliness, Repetition; and
    iii. Response Systems – IT systems, Manual Systems.
d. be conducted internally, while a review of a critical incident or major University-wide business disruption may be conducted by an independent external person / company.

Section 11 - Business Continuity and Resilience

(41) Business continuity is the management of the priorities, recovery procedures, responsibilities and resources that support the University and each individual business unit in managing recovery from a business disruption.

(42) In the event of a major Incident or Critical Incident, the University can implement business continuity and recovery management measures in addition to the Critical Incident processes identified in this Policy and its accompanying Procedure.

(43) Business resilience resources include:

a. Business Impact Assessment - identifies key internal systems, responsible staff, required equipment as well as allowable outage and recoverable time frames of all critical business processes across the University.
b. Business Continuity Plan - documents the priorities, procedures, responsibilities and resources that will support the business unit when managing a business disruption. Key inputs include the results of the BIA process, a threat assessment outlining credible disruption scenarios, and agreed response structures and strategies.
c. Business Recovery Plan - documents the priorities, recovery procedures, responsibilities and processes that will support the University in managing recovery from a major critical incident or business disruption. Key inputs include the results of the BIA process, response to Business Continuity Plans, recovery budget management etc.

Section 12 - Review

(44) This Policy and Critical Incident Management Procedure will be regularly reviewed to ensure they:

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

(45) Annual scenario exercises will be conducted to:

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

(46) Unless otherwise indicated, this Policy will still apply beyond the review date.

Section 13 - Further Assistance

(47) Please contact the Office of the Deputy Chief Operating Officer for any proposed changes or amendments.

Status and Details

Status	Historic
Effective Date	18th March 2024
Review Date	8th August 2028
Approval Authority	Vice-Chancellor and President
Approval Date	18th March 2024
Expiry Date	12th May 2024
Responsible Executive	Patrick Woods Chief Operating Officer
Responsible Manager	Paul Campbell Deputy Chief Operating Officer
Enquiries Contact	Gillian Rowlands Program Officer, Strategic Programs Office of the Deputy Chief Operating Officer