Critical Incident Management Procedure

Section 1 - Purpose

(1) This Procedure supports the [Critical Incident Management Policy](#).

(2) The purpose of this Procedure is to:

    a. support a timely and systematic response to Incidents and Critical Incidents;

    b. provide effective processes that support sound decision making;

    c. facilitate the effective co-operation between the University and Emergency Services;

    d. reduce the impact of an Incident or Critical Incident on people, property and the environment;

    e. improve the means by which the University manages information and communicates with stakeholders; and

    f. enable the recovery of critical business functions immediately following a disruption.

Section 2 - Principles

(3) The following principles should guide all actions when managing an Incident or Critical Incident:

    a. maintaining the safety and well being of students, employees, contractors, visitors and the community;

    b. maintaining public confidence and providing robust leadership for the University;

    c. protecting property, assets and the environment, complying with statutory obligations and optimising financial outcomes; and

    d. resuming business as usual as soon as possible, undertaking actions to prevent a reoccurrence and improving future responses.

Section 3 - Scope

(4) The scope of this Procedure extends to all areas and operations of the University.

(5) The [Critical Incident Management Policy](#) identifies three types of potential disruptions to the University: Events, Incident and Critical Incidents. Their definitions are provided in Section 5 – Incident Assessment Levels. This Procedure provides processes for the management of Incidents and Critical Incidents, not Events. An Event is managed on campus by local Emergency Services, Facilities Managers, State Facilities Manager, Security Managers and local resources.

Section 4 - Flowcharts

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the ACU Policy Portal for the latest version.

Page 1 of 13

Event, Incident and Critical Incident Flowchart

(6) The Event, Incident and Critical Incident Flowchart outlines how ACU responds to an Event, an Incident or a Critical Incident.

Incident Flowchart

(7) The Incident Flowchart outlines in further detail the processes for responding to an Incident.

Section 5 - Assessment

Incident and Critical Incident Assessment Categories

	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. 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. • 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.	Local responsible staff (e.g. first aid officers) Campus Facilities Emergency Services	Responses recorded as required in business as usual (BAU) processes and procedures.
Level 1	Incident	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. 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 resolved using normal operating procedures. • 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.	National Security Centre Incident Convenors	Incident Leads Incident Response Group Critical Incident Convenor External Regulators

Level		Criteria / Description	Responsible	Who to Notify
Level 2	**Critical Incident**	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. It requires a significant response and ongoing management. • 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.	Critical Incident Convenor	Vice-Chancellor and President Critical Incident Response Group (CIRG)

Incident and Critical Incident Codes

(8) 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	• 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	• Cyber Attack • Data / records loss • Business system failure • IT equipment failure • IT software failure
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 • Asbestos exposure

Colour Code	Type of Incident	Examples of Threats and Risks
Black	Personal Threat	• 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	• 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

Section 6 - Management

Incident Convenors

(9) Incidents are 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	Chief People Officer
Physical	Director, Properties and Facilities
Virtual	Chief Information and Digital Officer
Critical Incident Convenor	Deputy Vice-Chancellor (Corporate)

Incident Leads

(10) 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	Campus Dean Brisbane

Incident Leads	
Melbourne	Campus Dean Melbourne
North Sydney	Campus Dean North Sydney
Rome	Provost and Deputy Vice-Chancellor (Academic)
Reputation	Chief Marketing Officer
Fraud	Chief Financial Officer
Privacy	Director, Legal, Assurance and Governance
Sexual Assault / Harassment	Director, Student Experience and Enhancement
International	Pro Vice-Chancellor (Global and Education Pathways)
Student Accommodation	Director, Student Experience and Enhancement

Critical Incident Response Group

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

(12) CIRG will include officers of the University who can provide their expertise, resources and support in managing a Critical Incident. CIRG will oversee Critical Incident and recovery processes in conjunction with the Critical Incident Convenor.

Incident Response Group

(13) 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.

> See also the [Critical Incident Response Group Diagram](#).

Microsoft Groups Communication Tool

(14) The following Microsoft Groups have been pre-established to be used by Incident Convenors as needed to communicate information about a particular Incident.

(15) The groups are administered by the National Manager, Strategic Programs; the Program Officer, Strategic Programs, Office of Deputy Chief Operating Officer and each Executive Officer listed below. Administrators can add or remove staff from each Group or establish additional Groups as required. All members of a Group can directly email the Group.

(16) For the purposes of reporting and archiving, the Groups will be managed by:

a. National Manager, Strategic Programs; and
b. Program Officer, Strategic Programs.

(17) The five Groups are:

a. Critical Incident
b. Incident STUDENTS
c. Incident STAFF

    d. Incident PHYSICAL

    e. Incident VIRTUAL

(18) Each Group contains the following members:

    a. Deputy Vice-Chancellor (Corporate) (Critical Incident Convenor)
        i. Deputy Chief Operating Officer (Proxy)
        ii. Executive Officer, Chief Operating Officer

    b. Director, Student Administration (Incident STUDENTS Convenor)
        i. Associate Director, Student Systems (Proxy)
        ii. Executive Officer, Office of Director, Student Administration

    c. Chief People Officer (Incident STAFF Convenor)
        i. Associate Director, HR Business Partnering (Proxy)
        ii. Executive Officer, Office of Chief People Officer

    d. Director, Properties and Facilities (Incident PHYSICAL Convenor)
        i. Associate Director, Facilities Management (Proxy)
        ii. Executive Officer, Office of Director, Properties and Facilities

    e. Chief Information and Digital Officer (Incident VIRTUAL Convenor)
        i. Associate Director, IT End User Computing Services (Proxy)
        ii. Executive Officer, Office of Chief Information and Digital Officer

(19) Also included in each Microsoft Group are:

    a. Chief Marketing Officer (Incident Lead Reputation)
        i. Associate Director, Communication and Creative Services (Incident Lead Reputation proxy)

    b. Chief Financial Officer (Incident Lead Fraud)
        i. Associate Director, Financial Operations (Incident Lead Fraud proxy)

    c. General Counsel (Incident Lead Privacy)
        i. National Manager, Governance (Incident Lead Privacy proxy)

    d. National Manager, Strategic Programs, Office of Deputy Chief Operating Officer
        i. Program Officer, Strategic Programs, Office of Deputy Chief Operating Officer·

Section 7 - Command and Support Rooms

Command and Support Room Locations

(20) The following rooms (and buildings) are to be used as required during the management of an Incident or Critical Incident.

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of staff printing this document to always refer to the ACU Policy Portal for the latest version.   Page 6 of 13

Rooms Required	Primary Command Room	For use by the Critical Incident Convenor, Incident Convenor, Incident Lead and Incident Response Group while managing an Incident or Critical Incident
	Communications Team Room	During an Incident, this room will be used by the IRG Communications and Reputation Management Team to coordinate the communications aspects of an incident.
	Triage Area	Located close to one of the assembly areas – this room or area is private and has access to first aid equipment
	Family Reception Area	This area will be located away from the command and support rooms and be an area for family and friends to wait for situation updates
	Media Staging Area	This area is for external media personnel. This area should be located away from the command and support rooms and be an area for the media personnel to wait for media statements or conferences. Having an area will minimise the risk of media personnel accessing unauthorised areas of the campus.
Primary Command Room	Critical Incident	Apostolic Delegation Room 500.G.06 Vice Chancellery Building
	Ballarat	Torney Room 100.G.17 Carn Brea
	Brisbane	Room 200.2.23 Office of the Campus Dean (QLD)
	Canberra	Boardroom 301.1.18 Veritas Building
	Melbourne	IT Videoconference Room 464.2.07 174 Victoria Parade
	North Sydney	Room 529.3.17 21 Berry Street
	Strathfield	Videoconference room 600.1.02 Edmund Rice Building
Back-up Command Room - On Campus	Critical Incident	Videoconference Room 529.3.17 21 Berry Street
	Brisbane	Videoconference 212.2.19 Saint John Paul II
	Ballarat	Room 100.G.13 Office of the Campus Dean, Carn Brea
	Canberra	Boardroom 300.G.35 Blackfriars Building
	Melbourne	Callinan Board Room 460.8.57 250 Victoria Parade
	North Sydney	Apostolic Delegation Room 500.G.06 Vice Chancellery Building
	Strathfield	Videoconference 640.1.16 Clancy Building

Back up Command Room - Off Campus	Critical Incident	Dependent on location of Critical Incident
	Ballarat	Melbourne campus if required
	Brisbane	Level 3, Building 280 Brisbane Leadership Centre 229 Elizabeth St, Brisbane
	Canberra	Dickson College, Phillip Avenue Dickson
	Melbourne	Level 5, 215 Spring Street, East Melbourne
	North Sydney	Mary MacKillop Place, Mount Street North Sydney, or ACU Strathfield Campus
	Strathfield	Room 529.3.17, Level 3, 21 Berry Street North Sydney
Activation Procedure		1. Confirm room availability 2. Confirm equipment is available and set up 3. Liaise with administration and IT to provide any further required resources 4. Communicate relocation details to staff 5. Confirm room / building availability and resources for offsite locations if required

Command and Support Room Kits

(21) Each campus has physical kits that contain equipment and information to help manage an Incident or Critical Incident in the event that virtual communication is not possible. The kits are utilised when a Command Room is set up. The kits are supplied in a portable suitcase and should always be kept in the following locations:

Ballarat	• Office of Executive Officer to Campus Dean (Ballarat), Room, 100.G.12 (x2)
Brisbane	• Room 200.2.23, Office of the Campus Dean (QLD) • Room 200.1.21, Security Office • Room 212.G.26A, Store Room
Canberra	• Room, 301.1.18, Veritas Building, Office of the Campus Dean • Concierge Ground Floor, Blackfriars Building
Melbourne	• Room 411.G.01, Ground Floor, Office of the Campus Dean (VIC) • Brunswick Street, Fitzroy • Security Room, Ground floor Mary Glowrey Building (Building 420)
North Sydney	• Building 500 Reception, Vice-Chancellery • 532.G.01B Office of State Facilities Manager
Strathfield	• Facilities Management / Security Office • Room 613.1.30 Level 1, Office of Executive Officer, Campus Dean

Command and Support Room Equipment

Primary Command Room (including Critical Incident Command Room)	Room • Videoconferencing capability • Power board • Whiteboards x 2 • Flipchart / butchers paper • Large copies of University evacuation diagrams • Maps of local area	Support Kit / Suitcase • Incident management tabards and IRG member folders • Copy of Emergency Response Plan • Copies of this Procedure • IRG names and contact details • Incident videoconferencing details • IRG organisational wallchart • Copy of hazardous chemicals register • List of critical infrastructures • Stationery – pens, paper, markers, BlueTac, tape • Mobile phone chargers • Laptop chargers / powerpack

Communications Team Room	• Workstations • Printer • Mobile phone chargers • Whiteboard • Flipchart / butchers paper • Communications templates on USB • Stationery – pens, paper, markers	• Copy of this Procedure • Copy of Reputation Management Plan • Internal contact details • Media contact details
Triage Area	• Tarps / ground sheets • Blankets • Torches and glowsticks • Witches hats • Barrier tape • Pens, pencils, markers, paper • High vis vests • Water • Trauma first aid kits • Oxygen, spare masks and hoses • Defibrillator and spare pads	• Triage cards • PPE (gloves, masks, gowns, goggles, pocket masks) • Trauma shears • Garbage bags • Biohazard bags • Anti-bacterial wipes and gel • Sharps container for needles • Copy casualty register to record details and which hospital they were sent
Family Reception Area	• Large room, two smaller rooms, bathroom, kitchenette • High vis vest • Megaphone, if the space is large • First aid kit • Torch with batteries	• Pen and paper • Food, water, tea, coffee • Cups and appropriate kitchenware • Signage • Language translation cards

Media Staging Area	• USB and hard copy documentation:
	  ◦ Media Release
	  ◦ Media enquiry form
	  ◦ Media call log
	  ◦ Stakeholder lists
	  ◦ Holding statements
	• Large room, with nearby bathroom, and kitchenette, separate to family staging area
		• Lectern
		• Microphone
		• Pen and paper
		• Food, water, tea, coffee
		• Cups and appropriate kitchenware

Section 8 - Incident Staging Area Management

(22) ACU's Security, Emergency Wardens and Facilities Management teams will take initial control of the scene of a Physical Incident until the arrival of Emergency Services.

Actions

	Actions
1.	Confirm with the Emergency Coordinator where the Incident has occurred and where perimeters should be established.
2.	Retrieve Incident Control Point kit and take to Incident Control Point
3.	Ensure access to mobile phone (charged) and two-way radio
4.	Establish Incident scene containment: • Place barrier tape around inner cordon and outer cordon • Place signage for different areas within incident scene area • Ensure clear access for Emergency Services into incident area, and out of incident area
5.	Preserve the scene were possible for Police and Regulator investigations.

Containment

(23) The Incident scene may include a few different areas:

Hot Zone	Containing the immediate incident area to prevent people from entering. Only first responders should be in this area.
Warm Zone	Only internal response teams and Emergency Services should be in this area. When Emergency Services arrive, they will most likely contain the area further, and restrict access to only their teams.
Cold Zone	This area will be where the Emergency Services will establish their command post and coordinate their resources and equipment from.
Incident Control Point	Point where the Emergency Coordinator will generally coordinate the internal response teams from, and where they will meet external Emergency Services. This point will generally be just outside the cold zone.
ACU Staging Areas	Areas where people will meet. ACU should establish staging areas to manage large groups of persons. Some of these areas will be in conjunction with Emergency Services. Examples: media staging area, Emergency Services staging areas, triage areas, assembly points, family reception centre.

(24) See also the [Incident Scene Containment Set-up](#).

Resources

Resources needed	
• High vis vest and helmet / cap • First aid kit • Torch with batteries • Pen and paper • Blue tac • Flipchart paper and markers	• Megaphone • Barrier tape • Signage • Generators (if needed) • Portable lighting (if needed)

Section 9 - Acronyms

Type	Description
ACU	Australian Catholic University
BCP	Business Continuity Plan
CIRG	Critical Incident Response Group
DR	Disaster Recovery
EAP	[Employee Assistance Program](#)
ECO	Emergency Control Organisation
IAP	Incident Action Plan
IRG	Incident Response Group
NSC	National Security Centre
OHS	Occupational Health and Safety
PPE	Personal Protective Equipment
RFS	Rural Fire Brigade
SES	State Emergency Service
SLAIR	Security Logs and Incident Reporting
PIR	Post Incident Review
WHS	Work, Health and Safety
SITREP	Situation Report

Section 10 - Checklists

Incident Convenor

(25) [Incident Convenor Checklist](#)

(26) [Incident Convenor Impact Assessment Tool](#)

(27) [Incident Lead Checklist](#)

(28) [National Security Centre Checklist](#)

(29) [Support Coordinator Checklist](#)

(30) [People Coordinator Checklist](#)

(31) [Facilities Coordinator Checklist](#)

(32) [Communications Coordinator Checklist](#)

(33) [Business Continuity & Recovery Coordinator Checklist](#)

Section 11 - Specific Response Procedures and Actions

(34) [Active Shooter Checklist](#)

(35) [Asbestos Exposure Checklist](#)

(36) [Civil Unrest Checklist](#)

(37) [Construction Accident Checklist](#)

(38) [Cyber Attack Checklist](#)

(39) [Death of Staff or Student Checklist](#)

(40) [Environmental, Biological, Radiological, or Chemical Release Checklist](#)

(41) [Fire (major) Checklist](#)

(42) [Health Issue Disease Outbreak Checklist](#)

(43) [Improvised Explosive Device (IED) (in mass gatherings) Checklist](#)

(44) [Lost Group Checklist](#)

(45) [Mass Casualty Checklist](#)

(46) [Natural Disaster Checklist](#)

(47) [Sabotage of Critical Facility Checklist](#)

(48) [Serious Act of Violence Checklist](#)

(49) [Sexual Assault (including Allegations) Checklist](#)

(50) [Utility and IT Failure Checklist](#)

Section 12 - Business Resumption Checklist

(51) The business resumption strategy contains a series of actions and steps designed to return the affected campus to its pre-interruption status and should be conducted by the Business Continuity and Recovery Coordinator. This includes restoration or relocation of campuses and resumption of operations to maximum capacity. The business resumption strategy should commence as soon as possible without interfering with critical tasks or diverting key personnel from the initial recovery process.

(52) See the [Business Resumption Checklist](#).

Section 13 - Tools

(53) [Information Management – Visual Boards](#)

(54) [Post Incident Review (PIR)](#)

Forms and Templates

(55) [Initial Report Form](#)

(56) [Incident Log](#)

(57) [Incident Action Plan - Briefing Template](#)

(58) [Situation Report (SITREP)](#)

(59) [Debriefing Template](#)

(60) Meeting Agendas:

   a. [Incident Response Group Initial Team Meeting Agenda](#)
   b. [Ongoing Incident Response Group Meeting](#)
   c. [Shift Changeover Agenda](#)

(61) [People – Internal Team Tracking Log](#)

(62) [People – People at Risk Log](#)

(63) [People – Family Centre Register](#)

(64) [People – Casualty Register](#)

Status and Details

Status	Current
Effective Date	27th March 2024
Review Date	30th April 2024
Approval Authority	Vice-Chancellor and President
Approval Date	27th March 2024
Expiry Date	Not Applicable
Responsible Executive	Patrick Woods Deputy Vice-Chancellor (Corporate)
Responsible Manager	Paul Campbell Deputy Chief Operating Officer
Enquiries Contact	Gillian Rowlands Program Officer, Strategic Programs Office of the Deputy Chief Operating Officer