Institute of Advanced Research
The University for Innovation

Critical Incident Policy and Procedure

1. Policy

1.1 Introduction

The Institute of Advanced Research engages with a large number of staff, students, contractors, volunteers and visitors. It operates and participates in a broad range of activities across learning & teaching, research & innovation,. The University recognises that an incident or a critical incident may take place either on site or off-site, and may happen at any time of the day or night.

The Critical Incident Policy and Procedure 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 IAR and is subject to all applicable laws, regulations and codes.

This policy and its related procedures demonstrate IAR's commitment to:

- protecting the health and safety of staff, students, contractors, volunteers, visitors and the IAR community
- identifying and preventing incidents and critical incidents;
- ensuring business continuity;
- allocating appropriate resources and building relationships to manage incidents and critical incidents in compliance with IAR's mission, and legal obligations and standards;
- delivering the highest possible standard of health and safety for staff, students, contractors, volunteers, visitors, the IAR 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 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 obligations in relation to its staff, students, contractors, volunteers and visitors to ensure people are safe, and that IAR's reputation is maintained.

1.4 Critical Incident Policy

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

- Development, implementation and annual review of Critical Incident Management Procedures, as outlined under 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 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.

Nothing in this policy overrides the Code of Conduct for all staff, students or student conduct and discipline policis.

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.

1.7 Criterion for Activation of Critical Incident Procedures

The IAR Security will immediately notify the Campus Engineer, who will inform all Incident Response Group members when a situation is a potential Incident or Critical Incident.

The Campus Engineer, who is 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 lessons learned 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, the Campus Engineer, may initiate a recommendation for the Campus or Service to close, if closure has not been directed by Emergency Services.

The Registrar, following consultation with the President may approve the closure of a Campus or Service.

2. 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 IAR 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 IAR 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 IAR's people, operations, environment, its long-term prospects and/or its reputation. It requires a significant response and ongoing management.

2.2 Incident Categories

Due to the broad definition of what comprises a critical incident, IAR is committed to applying the International Coding of Incidents to increase its preparedness and the effectiveness of IAR's response and management of incidents. The Campus Engineer will manage an Incident, and initiate consultation with the Registrar, 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/utilitiesIT 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 Terrorism incident
Blue	Medical Emergency/Threat	Death staff / student Medical Emergency Poisoning

		Pandemic diseases Suicide
Black	Personal Threat	Active Shooter Assault Child protection matter Intrusion or hold-up Kidnapping Missing students / staff Attempted self-harm 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 Transport accident Severe weather and storms Supplier Failure Third party negligence

3. Critical Incident Team

3.1 Incident Response Group

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

3.2 Critical Incident Response Group

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

The Registrar 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 Campus Engineer of the Incident Response Group.

3.3 Communication

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

3.4 Accountabilities and Responsibilities

The Registrar, 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 Policy and Procedures.

The Registrar will raise awareness about the Critical Incident Policy and Procedures. IAR 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 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 Dean (Academic) and the HR Lead; 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.

4. 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 Registrar has delegated responsibility to make amendments to the Procedures.

5. 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 Enhancement of the Policy and Procedure

The policy will be reviewed by University Management Committee. Human Resources, Estates, and Marketing Leads – on an ongoing basis to improve its effectiveness.