Incident Management - Procedures

1. Purpose of procedures

1.1 The purpose of these procedures is to plan for, respond to, manage and escalate a Critical Incident quickly and effectively, bringing it under control, and limiting the impact to the University Community.

1.2 These procedures should be read in conjunction with the *Critical Incident Management – Governing Policy* and related documents.

2. Scope and application

2.1 These procedures are designed for the management of all incidents that have impacted upon or have the potential to impact the University Community, or the University's services and operations, property and the environment. These incidents include both physical actions or hazards and other forms which may cause major reputational damage or loss of University functions or operations. It applies to all UniSC campuses.

2.2 These procedures also apply to staff and/or students who are hosted at sites operated by Third-Party Providers, visiting other Third-Party Sites and on study tours or work placements.

2.3 All incidents will require response, notification, management, control, recording and closure as outlined below.

3. Definitions

Please refer to the University's Glossary of Terms for policies and procedures. Terms and definitions identified below are specific to these procedures and are critical to its effectiveness:

Australasian Inter-Service Incident Management System (AIIMS): a national system used by all emergency agencies and first responders when organising the managing of a disaster or emergency by function.

Business Continuity Plan (BCP): The University's plan that outlines how critical business operations can be maintained or recovered in a timely fashion.

Campus: means any campus or site owned or operated by the University.

Corrective action or Controls: action taken to improve the University's systems or processes to address non-conformance and/or eliminate or reduce risk.

Critical Incident: An incident that has a risk rating of extreme or high under the University's Risk Management Framework with a consequence of at least moderate. It requires a focused and concerted response and ongoing management by the Organisational Unit Manager in conjunction with the IRT.

Emergency Planning Committee (EPC): The EPC is established to ensure all applicable legislative requirements are met and sufficient resources (time, finance, equipment and personnel) are provided to enable the development and implementation of emergency (incident) plans in a multi-campus environment. This is a requirement of Australian Standard 3745-2010, *Planning for emergencies in facilities*. The EPC has broader planning responsibilities under the University's protection, resilience and sustainability system.

First Aid: Initial treatment for an injury which is normally given by a first aid officer.

Hazard: A source or a situation that has the potential to harm a person, the environment, cause damage to property, or a combination of these.

Incident: An incident is an issue that requires a response. An incident may impact on any area of University activity. An incident that is not considered to be critical has a localised containable impact and is unlikely to escalate in severity but requires response and management as part of ongoing business-as-usual.

Incident Response Team (IRT): A team of specialists that is mobilised to assess and respond to a significant incident that has occurred.

APPROVAL AUTHORITY

Vice-Chancellor and President

RESPONSIBLE EXECUTIVE MEMBER

Vice-Chancellor and President

DESIGNATED OFFICER

Chief Operating Officer

FIRST APPROVED

9 September 2008

LAST AMENDED

1 September 2020

REVIEW DATE

21 June 2025

STATUS

Active

University of the Sunshine Coast | CRICOS Provider Number: 01595D | Correct as at 9 May 2024

Medical treatment: treatment by a registered medical practitioner, paramedic or registered nurse practitioner.

Near miss: an incident that could have resulted in an injury or illness to people, danger to health, and / or damage to property or the environment, but did not.

Notifiable incident: an incident for which the University is legally required to notify State or Commonwealth government or a regulatory body.

Responsible officer/s (includes – SafeUSC /Manager/Supervisor/Academic staff member/Head of Work Unit/Executive Member): a person who has responsibility for others at work / study / research / field trip, volunteer, contractor activities and first aid duties. If there is no identifiable supervisor, (e.g. if the person involved is a member of the public, or a student not engaged in university activities) SafeUSC (Security) should be contacted. If the person involved is a contractor, their supervisor or manger is a person from where they are employed. SafeUSC is a primary point of contact for first aid in the case of an incident on campus.

Third-Party Providers: Organisations contracted by the University to provide services on its behalf (e.g. Australian Technical and Management College and cloud service providers).

Third-Party Sites: Sites that staff or students visit other than UniSC campuses and Third-Party Providers. This includes sites where staff and students are on work placements or study tours.

University Community: relates to students, staff and other stakeholders engaging with the University, including visitors, contractors and volunteers.

4. Procedures

4.1 Respond

4.1.1 Incident Response

An incident response can occur at any time and may be triggered from an alarm, conversation, email, phone call or a report.

The nature of the incident including the severity/consequence of an incident will determine the response required. Most incidents can and will be managed locally as part of a business-as-usual approach.

All incidents should be responded to with the following actions:

- ensure you protect your health and safety
- ensure you protect the health and safety of others, and if safe to do so, take appropriate action to make the area safe or to prevent any further likelihood of injury or illness
- if required, contact emergency services (000)
- if required contact SafeUSC on (+61) 7 5430 1168 or extension 1168
- if required, and if safe to do so, provide first aid to any other persons affected by or involved in an incident
- if safe to do so, activate standard operating procedures/processes to protect key assets, data and critical systems
- incidents of a confidential nature must only be shared/progressed with agreement and with authorised personnel (i.e. for student related incidents, these will be managed by Student Services and Engagement and will be escalated to the Director, Facilities Management for Critical Incidents and/or where required)
- if required, maintain communication with SafeUSC and/or emergency services
- if applicable, make notes of the incident such as names, location, time and a brief description of what occurred.

4.2 Notify

4.2.1 Notification requirements

For all incidents, once the initial incident response as per section 3.1 has been established, appropriate personnel or support services must be notified. Based on the severity of the incident (refer to Risk Management - Procedures) the following notification processes need to be actioned accordingly:

- Supervisor/s or a Responsible Officer must be notified as soon as possible if they have not yet been, except where there is a valid reason not to, for example, if the Supervisor/s or Responsible Officer is the subject of an allegation, or if they are absent.
- If required SafeUSC (Security) should be notified by calling (+61) 7 5430 1168 or by using one of the Emergency Call Points.
- Where a staff member requires additional support or assistance, HR should be notified by calling (+61) 7 5430 2820 or by email to hsw@usc.edu.au.
- Where a student requires additional support or assistance, Student Wellbeing should be notified by email to studentwellbeing@usc.edu.au.
- Where a contractor is involved in an incident, SafeUSC must be contacted on (+61) 7 5430 1168 or email fm@usc.edu.au.
- University insurance may need to be notified or referred on to for visitors and student incidents via email insurance@usc.edu.au.

- for all Critical Incidents IRT members must be notified (see Section 4.2.2).

Non-Critical Incidents are those that are considered minor in nature. If they relate to people, this includes most injuries that require limited first aid treatment and result in less than one week off work or study, lacerations, slips and trips, small or non-hazardous chemical spills that require in-house clean-up and short-term technological systems outages. Minor incidents can also relate to information technology, facilities/access such as a short-term power outage that is rectified quickly, or another incident that is not regarded as being high risk under the University's Risk Management Framework.

More serious non-critical incidents may be escalated to a Critical Incident response in accordance with the incident management decision tree process (Appendix 1) and will then require an IRT to be activated in accordance with Section 4.2.2.

4.2.2 Critical Incidents

Critical Incidents are actual or impending incidents that require ongoing management by an IRT. These incidents are typically of an emergency nature.

Examples of Critical Incidents may include, but are not limited to:

- a serious injury, illness or death;
- psychological episode involving students and/or staff;
- sexual and/or physical assault;
- kidnapping or hostage situation;
- major overseas events that may have an impact to the University Community;
- missing staff member or student;
- unplanned technological systems outage impacting critical systems;
- floods, fire or other extreme weather events;
- environmental hazard;
- chemical spill that requires involvement of external parties for clean-up/control, or requires closure of area other than the immediate area;
- breaches of information security;
- cyber security attack; and
- compliance breaches of high risk obligations.

When a Critical Incident has occurred, the people involved and/or a Responsible Officer/s must respond to the incident as per 3.1.1 and as soon as possible:

- activate emergency alarm/systems if required
- notify SafeUSC (+61) 7 5430 1168 or extension 1168, and emergency services on (000) if required
- notify Supervisor and/or Responsible Officer
- notify Director, Facilities Management and the IRT to facilitate the incident response. The Director, Facilities Management can be contacted on (+61) 7 5456 3567 or extension 3567.
- In the event of a serious or potentially serious safety incident involving members of the University Community, (see Appendix 2) requiring notification to WHSQ, contact HR immediately on (+61) 7 5430 2830 or by email to hsw@usc.edu.au.
- The Director, Facilities Management, as the IRT Leader, will inform the relevant members of the IRT and the Executive Liaison before convening an IRT. For student related incidents, the Pro Vice-Chancellor (Students) must be consulted on the management response approach.

The first formal meeting of the IRT should be held as soon as possible after the team has been mobilised.

The IRT will consist of nominated members of the University including:

- Director, Facilities Management (IRT Leader)*
- Chief Financial Officer (Deputy IRT Lead)
- Senior Manager, Security/SafeUSC
- Director, People and Culture
- Academic Registrar and Director, Student Services
- Director, Marketing
- Director, Governance and Risk Management

If a Critical Incident occurs at any campus or site other than the Sippy Downs campus, the Campus Manager is to be a member of the IRT.

Subject specialists may be appointed to the IRT depending on the nature of the incident. IRT subject specialists may provide information and assistance specific to the incident, which may include emergency management, safety, information technology, asset management, campus management, field work, human resources, crisis management, legal and emergency services.

Should the IRT Leader not be available, the Deputy IRT Lead will become the IRT Leader.

An incident report should be completed as soon as is reasonably practicable or at least within 24 hours. The extent of the University's insurer's liability to pay compensation may be limited where an incident notification of injury or illness is not received within 20 business days of becoming aware of the incident.

4.2.3 Notifiable incidents

Certain incidents are notifiable under relevant Commonwealth and/or State legislation. Incidents that are notifiable are required to be reported within required timeframes by the relationship manager for that regulator or government agency. For details as to who the relationship manager is, contact Legal Services or the Director, Governance and Risk Management.

A health and safety incident is notifiable if the incident involves workers or students and results in death, serious injury or illness of a person, or involves a dangerous incident with the potential to cause serious injury or illness.

For more information regarding 'notifiable incidents' see Appendix 2.

4.3 Manage

When an incident has occurred, the people involved and/or a Responsible Officer/s must, as soon as reasonably practicable, assess, refer or initiate:

- actions required to protect the health and safety of any persons affected by, involved or potentially involved in the incident;
- actions required to protect key assets, data and critical systems;
- additional actions or controls to be implemented to effectively manage the incident through to resolution and closure (e.g. localised incident management processes); and
- escalation of the incident to a critical response based on the severity/consequence (see Appendix 2).

In the case of a Critical Incident or a safety related notifiable incident, the area and/or any information should be preserved as much as possible for the purposes of any investigation.

4.3.1 Management of minor or non-critical incidents

Non-critical incidents should be managed within business-as-usual arrangements and/or through local incident management processes. Supervisors should be notified and additional support such as a first aid officer, technical, counselling or maintenance personnel requested as required.

4.3.2 IRT management of Critical Incidents

The IRT is responsible for the coordinated management of a Critical Incident and is normally mobilised as soon as possible following a Critical Incident in accordance with the *Critical Incident Management - Governing Policy*.

The IRT will assess and respond to the incident accordingly and will co-opt additional members, including subject specialists, as required and depending on the nature of the incident.

Specific tasks of the IRT include:

- evaluating the extent of the risk to University (staff, students, facilities, environment, reputation, etc.);
- developing strategies to manage the response to an incident with the immediate focus on containing the extent of the damage or incident;
- coordinating resources, including emergency services;
- liaising internally with Marketing to distribute consistent messages to the University Community and externally;
- liaising with external agencies/ organisations, including Federal/State/Local Disaster Management Groups;
- providing accurate and timely information to Executive staff if required; and
- initiating the Business Continuity Plan if necessary.

At certain times it might be appropriate to manage a Critical Incident under an alternative approach that is not a formal IRT. This may be appropriate in situations where the incident is confidential or sensitive in nature or for incidents where the consequence is moderate and it can be appropriately managed as part of Business as Usual. The IRT Leader will make this decision in consultation with the relevant operational area.

4.3.3 Student-related incidents

Where a student is involved in a Critical Incident and an IRT is activated, the Academic Registrar and Director, Student Services, as a member of the IRT, will advise the Pro Vice-Chancellor (Students) of the incident and the proposed response and the Pro Vice-Chancellor Student will be involved in the management of that response. The Academic Registrar and Director, Student Services / Pro Vice-Chancellor Students will be involved in any decision making around the management of that response through the operation of the IRT.

4.3.4 Activation of the University's Business Continuity Plan

Some Critical Incidents will require activation of the University's Business Continuity Plan (BCP). Activation of the University's BCP will be determined by the IRT. The IRT may activate the BCP if the incident has impacted or is reasonably certain to impact Critical Functions of the University for a time determined by the IRT to be unacceptable. For IT related incidents, the IRT will activate the BCP if the incident has impacted or is reasonably certain to impact Critical Functions of the University for greater than the maximum tolerable outage time.

4.4 Incident Control

During and following any incident, controls or corrective actions may need to be implemented to help resolve any immediate or residual physical, psychological, financial, environmental, reputational or social risk emanating from the incident.

Where possible, controls or corrective actions should be monitored to ensure they have been implemented correctly and a positive or effective outcome is achieved.

Where a near-miss or hazard is identified, the Responsible Officer/s and/or Supervisor or Organisational Unit Manager must, so far as reasonably practicable, consider, implement and record immediate corrective actions to be taken and additional controls required to prevent the possibility of an incident occurring.

4.5 Communication and record keeping

4.5.1 For all incidents

All records relating to incidents must be captured in an approved records management system, in accordance with the University's *Information and Records Management – Procedures*. The IRT Leader is responsible for ensuring record keeping is conducted in an approved format.

Hazards or residual risks, such as property or environmental damage that have the potential to cause injury, illness, or to affect core business facilities and services, are to be reported through the University's maintenance reporting system.

4.5.2 Confidentiality

The University generally will keep information it obtains in the course of risk assessments and management of incidents confidential. Confidential information will only be used for the purpose of risk assessment and the management of incidents.

Subject to limits of confidentiality (as per below), information about individuals will not be disclosed to any other person unless the individual concerned has given consent to its use. Release of information about an individual will normally require a written consent for disclosure, signed by the individual.

Limits of Confidentiality - Confidential information will be disclosed without the consent of the individual when:

- there exists a clear danger to the individual or to others; and/or
- there exists a legal requirement to do so.

4.5.3 IRT record keeping

Requirements regarding recording information during an incident (once an IRT is invoked) will be conducted in accordance with the procedures outlined in the IRT Support Manual.

4.6 Incident closure

Once an incident has been responded to in accordance with these procedures, the incident can be closed.

A review is required post-incident to ensure adherence to, and continuous improvement of, these procedures and any local operational process. It may also assist with ensuring all appropriate controls or corrective actions have been considered to prevent a recurrence of the incident. The review should also ensure the controls implemented have achieved the desired outcome and have not introduced additional hazards.

For Critical Incidents, the review may include an IRT debrief and an incident investigation.

4.6.1 IRT debrief

An IRT debrief is a debrief with IRT members relating to a Critical Incident that has occurred and how it was managed. An IRT debrief will be conducted within one week after the Critical Incident response ending and will involve all available IRT members. The debrief will be facilitated by the IRT Leader or delegate.

The debrief is to be undertaken to consider observations, insights, and processes, and to record learnings from the incident in such a way as to focus and understand:

- what went well (to be reinforced and highlighted);
- what needs amendment, adjustment;
- where there are gaps; and
- what needs to be created or fixed.

A summary of the debrief findings will be reported to the Emergency Planning Committee.

4.6.2 Incident investigations

An incident investigation is an investigation into the incident itself. An incident investigation aims to identify causal factors across the entire organisational system (e.g. communication, training, procedures, incompatible goals, equipment, etc.) which contributed to the incident (before, during and after) such as:

- people – e.g. documents and records, rosters, work history, physical and psychological state, ability, supervision, experience, training, communication, team cohesion
- equipment – e.g. design, construction, Personal Protective Equipment, testing, inspections, maintenance, modifications
- materials – e.g. hazardous substances, heavy loads
- environment– e.g. electricity, weather conditions, wind, noise, dust, pollution, vibration, wildlife, workplace layout and space
- processes – e.g. usage, content, format, review and monitoring, document control.

Critical Incidents will be investigated by the IRT unless it is deemed by the IRT Leader that an alternative approach is more appropriate.

The IRT Leader, in consultation with IRT members and appointed subject specialists, will determine the best approach for undertaking an investigation if required. Incident investigations should commence within 48 hours, or as soon as reasonably practicable, after the incident has occurred.

Non-Critical Incidents will be investigated in accordance with business as usual processes.

5. Responsibilities

ACTIVITY	UNIVERSITY OFFICER/COMMITTEE
Responsible and accountable to the Council for Incident Management.	Vice-Chancellor and President
Provide the Audit and Risk Management Committee with summary information concerning any Critical Incidents.	Director, Governance and Risk Management
Develop, implement, resource and maintain the protection, resilience, and sustainability system, including emergency plan, incident response procedures, and the readiness, training and awareness sessions for all persons responding to incidents and emergencies.	Chief Operating Officer
Trained in incident management procedures and prepared to convene an Incident Response Team to evaluate and manage incidents across campuses.	Key Management Personnel. Key Management Personnel are required to nominate an appropriate delegate who will be trained to manage an IRT in their absence.
Advise staff within their area of responsibility of this procedure and its associated policy on a regular basis.	Organisational Unit Managers
Responsible for the administration of the University *Critical Incident Management – Governing Policy.*	Chief Operating Officer
Responsible for assessing incidents that are escalated and advising on the notification requirements.	University Risk Management Committee and/or Regulatory Relationship Manager
Act as Incident Controller for a significant incident or for Local/District Disaster Management responses.	Director, Facilities Management or Senior Manager, Security/SafeUSC
Develop and maintain close liaison with relevant Intelligence and Government Agencies, Queensland Police Services, other Emergency Response Services and Disaster Management Groups to ensure an effective notification, alert, support and response to	Senior Manager, Security/SafeUSC or delegate

potential or actual University incidents. Regulatory relationship management with the University's regulators (including but not limited to the Office of the Information Commissioner, WorkSafe and the Tertiary Education Quality Standards Agency) remain the responsibility of the designated staff member within each relevant area.	
Ensure students receive information about this policy and its associated procedures as part of their induction or orientation to the University.	Academic Registrar and Director, Student Services
Ensure staff receive information about this policy and its associated procedures as part of their induction or orientation to the University.	Director, People and Culture
Notified of all student related incidents, informed about all significant student-related incidents, consulted prior to IRT and involved in the management of all critical student related incidents.	Pro Vice-Chancellor (Students)
Ensure staff and students on field trips or study tours are prepared for any incident in terms of orientation, induction, in-country briefings, incident responses, host nation contacts and third-party emergency contact in country of activity.	Heads of School

Appendix 1 – Escalation Pathway for incidents

Appendix 2 – Health and Safety 'Notifiable Incident'

* For cyber-related incidents, the IRT Leader will be the Director, Information Technology.

END

RELATED DOCUMENTS

- Critical Incident Management - Governing Policy

- Health, Safety and Wellbeing - Governing Policy
- ICT Security - Operational Policy
- Resolution of Complaints (Staff) - Guidelines
- Risk Management - Governing Policy
- Risk Management - Procedures
- Staff Code of Conduct - Governing Policy
- Student Conduct - Governing Policy

LINKED DOCUMENTS

- Critical Incident Management - Governing Policy

SUPERSEDED DOCUMENTS

- Critical Incident Management - Procedures

RELATED LEGISLATION / STANDARDS

- University of the Sunshine Coast Act 1998 (Qld)
- Privacy Act 1988 (Cth)
- Education Services for Overseas Students (ESOS) Act 2000 (Cth)
- Work Health & Safety Act 2011 (Qld)
- Building Fire Safety Regs 2008
- National Code of Practice for Providers of Education and Training to Overseas Students 2018
- Information Privacy Act 2009 (Qld)
- Workers' Compensation and Rehabilitation Act 2003 (Qld)
- AS 3745 -2010 Emergency control organisation and procedures for buildings, structures and workplaces
- Fire & Emergency Services Act 1990
- Environmental Protection Act 1994
- AS ISO/IEC 27035 IT - Security techniques - Information security incident management
- Disaster Management Act 2003 (Qld)