

Critical Incident Policy and Procedures

Purpose

This Policy specifies the Institute's approach to managing critical incidents by providing a framework that integrates with the Institute's Risk Management Framework and aligns with the Higher Education Standards Framework (Threshold Standards) 2021 and ESOS National Code. It supports systematic and effective approaches to managing incidents that may seriously affect the Institute's staff, students, visitors, property, operations, activities, or reputation, ensuring their health, safety, and security. Additionally, the Policy includes a process for evaluating the Institute's responses to critical incidents to continuously improve response strategies and staff capabilities.

Scope

This Policy applies to all staff, students, visitors, and contractors at the Institute.

Related Documents

This policy should be read in conjunction with the following Institute documents:

- Information and Privacy Policy and Procedures
- Information and Records Management Policy and Procedures
- Intellectual Property Policy and Procedures
- Financial Controls Policy and Procedures
- Data Protection and Data Privacy Management Policy

- Risk Management Policy and Procedures
- Work Health and Safety Policy and Procedures
- Fraud, Corruption and Mismanagement Policy

All documents referenced in this policy can be accessed via the CITI website.

Definition of Key Terms

For the purpose of this Policy, the following definitions apply:

Term	Definition
Critical Incident	A critical incident is any event, sudden or unexpected, that causes or has the potential to cause physical or psychological harm, threatens life, safety, or wellbeing, or significantly disrupts the operations, learning, or work environment of the Institute. Critical incidents may include, but are not limited to, accidents, natural disasters, medical emergencies, violent acts, sexual assault or sexual harassment (SASH), or events that attract regulatory or public attention. Critical incidents require an immediate and coordinated response to protect individuals and meet legislative and regulatory obligations under the ESOS Act 2000, the National Code of Practice 2018, and the Threshold Standards 2021
Psychological Incident	A psychological incident is any event, including but not limited to critical incidents, that causes or may cause emotional or mental distress to students, staff, or other members of the Institute community. This includes exposure to trauma, threats, harassment, or incidents resulting in fear, anxiety, or other adverse mental health outcomes. The Institute is committed to

Term	Definition
	identifying, monitoring, and supporting individuals affected by psychological incidents in line with its duty of care and regulatory obligations.
Sexual Assault and Sexual Harassment (SASH) Incident	A SASH incident refers to any act of sexual assault, sexual harassment, or gender-based violence that occurs within the context of the Institute's operations or impacts its community. Such incidents may constitute critical incidents where immediate intervention is required to ensure safety and wellbeing. SASH incidents are managed in accordance with the Institute's SASH Policy and Procedures, and all mandatory reporting, support, and investigation requirements under the ESOS Act 2000, National Code, and relevant Australian legislation are strictly followed.
Incident Management Team (IMT)	Incident Management Team (IMT) means a group of trained and competent Institute staff members responsible for managing the Institute's strategic response to critical incidents.
Wellbeing	Wellbeing refers to the holistic physical, psychological, emotional, and social health of students, staff, and other members of the Institute community. In the context of critical incident management, wellbeing encompasses the Institute's proactive and responsive measures to prevent harm, provide support, and facilitate recovery, ensuring individuals can safely continue their learning, work, or participation in Institute activities.
Mandatory Reporting	Mandatory reporting is the legal or regulatory obligation to notify relevant authorities of certain incidents or risks

Term	Definition
	<p>affecting students or staff, including critical incidents, SASH incidents, notifiable work health and safety events, or circumstances affecting compliance with visa conditions. Mandatory reporting under the ESOS Act 2000, the National Code 2018, and WHS legislation ensures that the Institute informs regulators such as TEQSA, SafeWork NSW, the Department of Home Affairs, and other authorities as required to maintain safety, compliance, and student protection.</p>
<p>Provider Registration and International Student Management System (PRISMS)</p>	<p>PRISMS reporting refers to the Institute's obligation to record and submit information about overseas students' enrolment, attendance, course progress, and critical incidents via PRISMS as required under the Education Services for Overseas Students (ESOS) Act 2000 and the National Code of Practice for Providers of Education and Training to Overseas Students 2018. PRISMS reporting ensures that the Institute protects the rights, wellbeing, and safety of international students by monitoring compliance with visa conditions, course progress, attendance, and the timely management of critical incidents, including those that may affect students' physical or psychological health. The system also facilitates mandatory notification to the Department of Home Affairs, supporting regulatory oversight and safeguarding students' legal and educational entitlements.</p>

Policy Principles

The Institute's critical incident management capability is guided by the following principles, ensuring a comprehensive, proactive, and student-centred approach to safety, wellbeing, and operational resilience:

1. **Planning and Preparedness:** Establishing, documenting, and maintaining clear procedures for the prevention, management, and escalation of critical incidents. Ensuring all staff and students are trained and aware of their roles and responsibilities in the event of a critical incident. Conducting regular testing, drills, and scenario planning to validate readiness and refine emergency procedures.
2. **Risk Identification and Mitigation:** Proactively identifying potential hazards, threats, and vulnerabilities that may lead to physical or psychological harm. Assessing, prioritising, and implementing control measures to reduce risk to individuals, assets, and institutional operations. Continuously monitoring risks and updating mitigation strategies in line with regulatory and legislative requirements.
3. **Response:** Acting immediately to protect life, health, and wellbeing, including psychological safety, during a critical incident. Coordinating the Incident Management Team (IMT) to manage operational, academic, reputational, and strategic consequences. Communicating effectively with affected individuals, staff, regulators, and relevant authorities to ensure informed decision-making.
4. **Recovery and Continuity:** Implementing business continuity arrangements to restore essential functions and services following a critical incident. Providing ongoing support to affected individuals, including counselling, academic accommodations, and follow-up care. Addressing physical, psychological, operational, and reputational impacts to stabilise the Institute and minimise disruption.
5. **Learning and Continuous Improvement:** Reviewing and analysing all critical incidents to identify lessons learned, systemic weaknesses, and areas for improvement. Updating policies, procedures, training, and risk management



strategies based on incident reviews. Promoting a culture of resilience, proactive risk management, and continuous enhancement of the Institute's critical incident capability.

Policy Statement

1. Legislative Requirements

- 1.1 The Institute is committed to ensuring the safety, wellbeing, and protection of all students, staff, and visitors. In accordance with the Education Services for Overseas Students (ESOS) Act 2000, the National Code of Practice for Providers of Education and Training to Overseas Students 2018, and the Higher Education Standards Framework (Threshold Standards) 2021.
- 1.2 The Institute recognises that critical incidents are events that may cause significant physical or psychological harm, and require an immediate, coordinated, and compassionate response.
- 1.3 The Institute will maintain robust procedures to prevent, prepare for, respond to, and recover from critical incidents, ensuring that affected individuals receive timely support, including access to emergency services, counselling, medical care, and other relevant assistance.
- 1.4 The Institute will also meet all reporting obligations to regulators and relevant authorities.

2. Types of Critical Incidents

A critical incident is any sudden or unexpected event that has the potential to cause serious physical or psychological harm, threatens life or safety, or significantly disrupts the operations of the Institute. This includes, but is not limited to:



- 2.1 Life-threatening events, such as fire, explosion, chemical spill, gas leak, electrical failure, violent attack, active shooter or terror incident, fatality, serious injury, missing persons, epidemic, or natural disaster.
- 2.2 Psychological or wellbeing-related incidents, including threats of self-harm or harm to others, severe mental health episodes, traumatic events affecting students or staff, or any situation where a person's psychological safety is at immediate risk.
- 2.3 Critical operational or reputational incidents, such as cyber-attacks, significant data breaches, fraud or mismanagement, criminal activity, or events likely to attract adverse attention from government agencies, regulators, interest groups, the public, or media.

3. Governance

The Institute maintains a comprehensive governance framework to ensure that all critical incidents are managed in accordance with the ESOS Act 2000, the National Code of Practice for Providers of Education and Training to Overseas Students 2018, the Work Health and Safety Act 2011 (NSW), and the Higher Education Standards Framework (Threshold Standards) 2021. This framework ensures effective oversight, accountability, and transparency across all levels of governance.

- 3.1 **Work Health and Safety (WHS) Committee:** The Work Health and Safety (WHS) Committee, chaired by the General Manager Operations, or delegate, provides operational oversight of health, safety, emergency management, and incident preparedness. The WHS Committee is responsible for:
 - 3.1.1 Maintaining and reviewing the Institute's Emergency Management Framework.
 - 3.1.2 Overseeing emergency planning, risk assessments, staff training, and compliance with WHS legislation.



- 3.1.3 Reviewing critical incidents to ensure continuous improvement and the implementation of corrective actions.
- 3.1.4 Escalating WHS concerns, systemic risks, and significant incidents to the Audit and Risk Committee.
- 3.2 **Audit and Risk Committee:** The Audit and Risk Committee provides institutional oversight of risk management and compliance related to critical incidents. The Committee:
 - 3.2.1 Receives reports from the WHS Committee, the Incident Management Team, and Operations.
 - 3.2.2 Reviews systemic, operational, reputational, and financial risks associated with critical incidents.
 - 3.2.3 Ensures that risk mitigation strategies, business continuity arrangements, and internal audit mechanisms are robust and effective.
 - 3.2.4 Advises the Board of Directors on significant incidents, emerging risks, and required actions.
 - 3.2.5 Ensures critical incident learnings are incorporated into the institutional risk register.
- 3.3 **Academic Board:** The Academic Board monitors academic risk and the impact of critical incidents on learning, teaching, assessment, academic integrity, and student progression. The Academic Board:
 - 3.3.1 Reviews reports on critical incidents that affect academic operations or academic wellbeing.
 - 3.3.2 Ensures that academic policies, student support processes, and continuation strategies remain responsive to incidents that impact student learning.
 - 3.3.3 Advises the Board of Directors on academic risks arising from critical incidents and the adequacy of institutional academic responses.

- 3.4 **Board of Directors:** The Board of Directors holds ultimate governance responsibility for oversight of critical incident management. The Board:
 - 3.4.1 Receives escalated reports from the Audit and Risk Committee and the Academic Board.
 - 3.4.2 Ensures that the Institute maintains a safe environment, robust governance framework, and compliance with all regulatory obligations.
 - 3.4.3 Monitors the strategic implications of critical incidents, including impacts on operations, student safety, institutional reputation, and regulatory standing.
 - 3.4.4 Approves major updates to emergency management and critical incident policies.
- 3.5 **Reporting to Relevant Bodies:** The Institute will comply with all statutory and regulatory reporting requirements arising from a critical incident. All external reporting will be timely, accurate, and documented. The General Manager Operations coordinates regulatory reporting unless delegated to another authorised officer.
 - 3.5.1 Depending on the nature and severity of the incident, reporting may be made to:
 - 3.5.2 Police, ambulance, and fire and rescue services
 - 3.5.3 SafeWork NSW
 - 3.5.4 TEQSA
 - 3.5.5 The Department of Home Affairs (via PRISMS for overseas students)
 - 3.5.6 Insurers
 - 3.5.7 Other authorities as required by law or contractual obligations



- 1.1 **Executive Oversight:** The Incident Management Team (IMT) is responsible for managing the Institute's operational response. Governance committees provide oversight, risk management, and assurance to the CEO and the Board of Directors. The CEO will be informed of all critical incidents classified as significant or requiring external reporting.

4. Incident Management Team (IMT)

The Institute will maintain a trained and competent Incident Management Team (IMT) responsible for coordinating the Institute's strategic response to any critical incident.

- 4.1 The IMT provides executive decision-making, ensures the safety and wellbeing of all affected persons, and oversees internal and external communications, support services, recovery planning, and reporting to regulators where required. The IMT comprises:
- 4.1.1 General Manager Operations (Chair)
 - 4.1.2 Chief Executive Officer (ex officio)
 - 4.1.3 Quality and Compliance (ex officio)
 - 4.1.4 Registrar
 - 4.1.5 Dean
 - 4.1.6 Relevant staff members

5. Incident Classification and Escalation

The Institute uses a risk-based, critical incident classification and escalation process in alignment with the Institute's Risk Assessment Matrix to define the level of response required to manage incidents:

- 5.1 **Level 1 (Minor) Incident:** Has no more than a minor impact rating in any risk category and little or no potential to escalate.



- 5.1.1 Can be resolved satisfactorily through standard procedures and channels.
- 5.1.2 Can be managed satisfactorily at the local level by on-site personnel, which may include an Incident Management Team (IMT) if the incident is an emergency.
- 5.2 **Level 2 (Moderate) Incident:** Has no more than a moderate impact in any risk category but has the potential to escalate.
 - 5.2.1 May not necessarily be resolved satisfactorily by standard procedures and channels.
 - 5.2.2 Needs moderate levels of resource and input to manage, which may include a business continuity response and, if the incident is an emergency, an IMT.
- 5.3 **Level 3 (Critical) Incident:** Has a substantial, major, or catastrophic impact rating in any risk category and will be an event or issue that:
 - 5.3.1 Has a long-term or profound effect.
 - 5.3.2 Cannot be controlled through standard procedures and channels.
 - 5.3.3 Needs high levels of resources and inputs to manage, which will include the IMT and may include a Business Continuity response as directed by the Chief Executive Officer and Board of Directors.

6. Managing Psychological Harm

The Institute recognises that critical incidents may cause not only physical harm but also psychological or emotional distress to students, staff, and other members of the Institute community.

- 6.1 In line with Standard 9.30 of the National Code and relevant Threshold Standards, the Institute is committed to identifying, mitigating, and supporting all individuals affected by psychological harm arising from critical incidents.



- 6.2 **Identification of Psychological Harm:** Critical incidents that may result in psychological harm include, but are not limited to:
- 6.2.1 Threats to life or personal safety.
 - 6.2.2 Traumatic events, such as accidents, violence, or self-harm.
 - 6.2.3 Exposure to distressing incidents involving colleagues, peers, or the wider community.
 - 6.2.4 Events that significantly disrupt study, work, or normal routines.
 - 6.2.5 Staff and students are encouraged to report concerns regarding emotional or psychological distress to the Incident Management Team (IMT) or designated student support officers.
- 6.3 **Immediate Response and Support:** The IMT will prioritise the safety and psychological wellbeing of affected individuals alongside physical safety.
- 6.3.1 Immediate actions may include:
- Ensuring the individual is removed from immediate danger or stressors
 - Providing access to professional counselling, mental health services, or employee assistance programs
 - Arranging peer or supervisor support where appropriate
 - Coordinating with external agencies, including medical or mental health services, where required
- 6.4 **Ongoing Monitoring and Assistance:** The Institute will provide ongoing support to affected individuals following a critical incident.
- 6.4.1 The WHS Committee, in conjunction with the IMT and Student Support Services, will monitor the wellbeing of those impacted and coordinate interventions as needed.
- 6.4.2 Individual support plans may include:
- Referral to professional psychological services



- Temporary adjustments to study, work, or duties to reduce stress
- Follow-up check-ins to assess recovery and readiness to resume normal activities
- 6.5 **Documentation and Reporting:** All incidents involving potential psychological harm will be documented in accordance with the Institute's recordkeeping and privacy policies.
 - 6.5.1 Reports will include the nature of the incident, individuals affected, interventions provided, and outcomes of any follow-up support.
 - 6.5.2 Significant incidents or repeated psychological harm events will be reported to the WHS Committee, Audit and Risk Committee, and, where required, to external regulatory authorities, including TEQSA.
- 6.6 **Preventive Measures and Training:** The Institute is committed to reducing the likelihood of psychological harm by:
 - 6.6.1 Embedding mental health and wellbeing considerations into risk assessments and emergency planning.
 - 6.6.2 Providing staff training on recognising and responding to psychological distress.
 - 6.6.3 Maintaining clear procedures for escalation and support during and after critical incidents.

7. Managing Sexual Assault and Sexual Harassment (SASH) Incidents

The Institute recognises that critical incidents may include situations involving sexual assault, sexual harassment, or other forms of gender-based violence, which can cause both physical and psychological harm. The wellbeing and safety of students, staff, and other members of the Institute community are paramount in all responses.



- 7.1 **Alignment with the SASH Policy:** All incidents of sexual assault or sexual harassment are managed in accordance with the Institute's Sexual Assault and Sexual Harassment (SASH) Policy and Procedures.
- 7.1.1 Staff, students, and visitors involved in, or witnessing, such incidents must follow the reporting, support, and response processes outlined in the SASH Policy.
- 7.1.2 The SASH Policy provides guidance on immediate safety, counselling support, investigation procedures, and reporting obligations.
- 7.2 **Immediate Response:** Any individual affected by a SASH incident should be prioritised for immediate safety and wellbeing.
- 7.2.1 The Incident Management Team (IMT), in coordination with Student Services and relevant support staff, will ensure:
- Protection from further harm or harassment
 - Access to medical care, counselling, and psychological support
 - Confidentiality and respectful handling of all parties involved
- 7.3 **Reporting and Regulatory Obligations:** SASH incidents are reported in accordance with the SASH Policy and any mandatory reporting requirements under the law, including TEQSA and other relevant regulatory authorities.
- 7.3.1 The Institute maintains accurate documentation of all reported SASH incidents and interventions while protecting the privacy of affected individuals.
- 7.3.2 Significant incidents are escalated to the WHS Committee, Audit and Risk Committee, and the Board of Directors as appropriate.
- 7.4 **Ongoing Support and Monitoring:** The Institute provides ongoing support to individuals affected by SASH incidents, including access to counselling, academic adjustments, and other reasonable accommodations.



- 7.4.1 Follow-up measures are monitored by Student Services in consultation with the IMT to ensure recovery and safety.
- 7.5 **Integration with Critical Incident Management:** SASH incidents are treated as critical incidents where appropriate and are incorporated into the Institute's Critical Incident Policy and Procedures framework.
- 7.5.1 All actions taken align with legislative requirements, the National Code, and the Threshold Standards, ensuring that the wellbeing, safety, and dignity of affected individuals remain the highest priority.

Procedures

These procedures give effect to the Critical Incident Policy and are aligned with work health and safety legislation and the Institute's commitment to student wellbeing and safety.

1. Planning and Preparation

The Institute adopts a proactive approach to planning and preparing for critical incidents to minimise risk and ensure a timely, coordinated response.

- 1.2 The WHS Committee has oversight of planning and preparedness activities, including the development, implementation, and maintenance of Critical Incident Management Plans.
- 1.3 Critical Incident Management Plans will:
 - 1.3.1 Identify potential critical incidents, including those impacting student safety, welfare, and visa status.
 - 1.3.2 Outline roles, responsibilities, communication protocols, and escalation pathways; and



- 1.3.3 Incorporate specific considerations for international students in accordance with the ESOS Act and National Code.
- 1.4 Staff, contractors, and relevant affiliates will receive regular training on emergency procedures, critical incident response, and their obligations under this Policy.
- 1.5 The Institute will conduct regular drills, simulations, and scenario testing to assess preparedness and ensure staff are familiar with response procedures.

2. Detecting and Mitigating Critical Incidents

The Institute actively monitors and manages risks to prevent or reduce the likelihood and impact of critical incidents.

- 2.1 The WHS Committee has oversight of systems used to identify, assess, and monitor potential critical incidents, including academic, welfare, health, safety, and security risks.
- 2.2 Risk assessments will be conducted regularly and updated when new risks are identified or when changes occur to operations, student cohorts, or the external environment.
- 2.3 Controls and mitigation strategies will be implemented to reduce identified risks, including preventative wellbeing measures, safety controls, and early intervention strategies for students at risk.

3. Responding to a Critical Incident

The Institute will respond promptly, compassionately, and effectively to all critical incidents, with student safety and wellbeing as the highest priority.

- 3.1 Upon identification of a critical incident, the Incident Management Team (IMT) will be activated without delay.



- 3.2 The IMT will:
 - 3.2.1 Ensure the immediate safety and wellbeing of students, staff, and visitors.
 - 3.2.2 Provide or arrange emergency assistance as required, including medical, police, or other emergency services.
 - 3.2.3 Manage communications internally and externally, including with students, families (where appropriate), and relevant authorities.
 - 3.2.4 Ensure international student obligations under the ESOS Act and National Code are met, including appropriate support and reporting where required.
- 3.3 Reasonable steps will be taken to minimise damage to Institute assets, operations, and reputation while maintaining a focus on human safety and welfare.
- 3.4 All actions taken during the response will be documented in accordance with records management requirements.

4. Student Wellbeing and Support

Student wellbeing is central to the Institute's critical incident response.

- 4.1 The Institute will provide timely and appropriate support to affected students, which may include:
 - 4.1.1 Counselling or referral to external professional support services.
 - 4.1.2 Academic flexibility or reasonable adjustments.
 - 4.1.3 Welfare checks and ongoing case management.
 - 4.1.4 Assistance for international students in understanding visa, enrolment, or reporting implications.
- 4.2 Where an incident affects an international student's enrolment status, Confirmation of Enrolment (CoE), or visa conditions, the Institute will



manage all reporting obligations in accordance with the ESOS Act and National Code.

- 4.3 Support will be offered in a culturally sensitive manner and tailored to the individual needs of the student.

5. Recovery and Business Continuity

Following the immediate response, the Institute will focus on recovery and continuity of operations.

- 5.1 The Chief Executive Officer, in consultation with Operations, Quality and Compliance, Dean, and the Board of Directors, will activate Business Continuity Plans as required.
- 5.2 Recovery actions may include:
 - 5.2.1 Restoration of facilities, systems, or services.
 - 5.2.2 Ongoing wellbeing and counselling support.
 - 5.2.3 Academic and operational adjustments to minimise disruption to students.
- 5.3 The Institute will communicate clearly with affected stakeholders throughout the recovery phase.

6. Learning, Review, and Continuous Improvement

The Institute is committed to learning from critical incidents to strengthen future preparedness.

- 6.1 The WHS Committee will oversee post-incident reviews to evaluate the effectiveness of the response and identify areas for improvement.



- 6.2 Outcomes of reviews may include updates to policies, procedures, training programs, or risk management strategies.
- 6.3 Lessons learned will be incorporated into future planning and staff training to continuously improve critical incident management capability.

7. Reporting and Accountability

- 7.1 All critical incidents must be reported immediately through the Institute's reporting channels.
- 7.2 The IMT will ensure that a thorough investigation is conducted, appropriate actions are implemented, and internal escalation occurs in line with governance and risk frameworks.
- 7.3 Where a critical incident affects, or has the potential to affect, students' enrolment, safety, welfare, academic progress, or visa status, the Institute will assess and meet all external reporting obligations, including reporting to TEQSA and other relevant regulators where required.
- 7.4 For international students, reporting obligations under the ESOS Act and National Code, including PRISMS reporting, will be managed accurately and in a timely manner.
- 7.5 A Critical Incident Report Form (Appendix 1) and/or Accident Investigation Report (Appendix 2) must be completed within timeframes appropriate to the nature and severity of the incident.
- 7.6 Records relating to critical incidents will be maintained in accordance with the Institute's Information and Records Management Policy and Procedures and will be available for regulatory review if required.



8. Confidentiality and Privacy

- 8.1 All information relating to critical incidents will be handled sensitively and confidentially.
- 8.2 Personal information will be managed in accordance with privacy legislation and the Institute's Information and Privacy Policy and Procedures.
- 8.3 Information will only be disclosed where necessary to protect health and safety, meet legal obligations, or support affected individuals.

9. Roles and Responsibilities

- 9.1 **Shareholders:** Support a governance framework that prioritises safety, wellbeing, and regulatory compliance.
- 9.2 **Board of Directors:** Provide strategic oversight of critical incident management and ensure compliance with legislative and regulatory obligations.
- 9.3 **Academic Board:** Oversee academic integrity and academic continuity considerations arising from critical incidents.
- 9.4 **WHS Committee:** Oversee preparedness, risk management, incident review, and continuous improvement.
- 9.5 **Audit and Risk Committee:** Provide independent oversight of critical incident management, risk controls, and compliance. Monitor significant critical incidents and emerging risks, including those impacting student safety, welfare, or regulatory obligations. Review post-incident reports, assurance activities, and management responses. Escalate material risks or systemic issues to the Board of Directors as required.



- 9.6 **Chief Executive Officer (CEO):** Lead the Institute's response to critical incidents and ensure appropriate resources, reporting, and support are in place.
- 9.7 **Operations:** Coordinate operational response, facilities management, and business continuity actions.
- 9.8 **Quality and Compliance:** Ensure compliance with the ESOS Act, National Code, TEQSA requirements, and internal policies.
- 9.9 **Dean:** Manage academic impacts, student support measures, and liaison with academic staff.

10. Review

These procedures will be reviewed annually by the WHS Committee, or earlier if required due to legislative changes, regulatory guidance, or following a critical incident.

Related Legislation

This policy should be read in conjunction with the following related documents:

- [Higher Education Standards Framework \(Threshold Standards\) 2021](#)
- [Education Services for Overseas Students Act 2000](#)
- [Australian Qualifications Framework](#)
- [Commonwealth Ombudsman](#)
- [Commonwealth Fair Work Act 2009](#)
- [Work Health and Safety Act 2011](#)
- [Work Health and Safety Regulation 2017](#)
- [Work Health and Safety Codes of Practice](#)
- [National Employment Standards \(NES\)](#)



Change and Version Control

Version	Date Approved	Authored by	Approved by	Description
1.0	11/09/2024	Chief Executive Officer	Board of Directors	Corporate Policy

Policy Information

Author	Chief Executive Officer
Responsible Officer	Chief Executive Officer
Approved by	Board of Directors
Approval Date	11/09/2024
Status	Approved (Current Version)
Next review due	11/09/2027

Name of Policy	Critical Incident Policy and Procedures		
Version	V1.0		
Policy: Corporate	Date: 11/09/2024	Status: Final ratified by the Board of Directors on 11/09/2024	

File: Critical Incident Policy and Procedures_V1.0

Appendix 1: Critical Incident Report Form

It is important to approach the situation with sensitivity and a focus on the welfare of the injured staff member, student, or visitor while also taking steps to prevent similar incidents in the future. Compliance with WHS legislation and continuous improvement of safety practices are essential for protecting all employees. Please fill out this form completely and submit it to the Director of Quality and Compliance as soon as possible after the incident occurs. For any questions or further assistance, contact the Director of Quality and Compliance.

Section 1 – General Information	
Ensure the critical incident report is a comprehensive and detailed aid in understanding the sequence of events, identifying the root causes, and implementing effective preventative measures. It also serves as a legal document that can be crucial for insurance claims, regulatory compliance, and defending against potential lawsuits.	
Date and Time:	(When the incident occurred.)
Location:	(Where the incident happened, with as much detail as possible.)
Reporter's Details:	(Name, position, and contact information of the person reporting the incident.)
Involved Parties:	(Names and roles of all individuals involved, including witnesses.)
Contact information:	(For those involved, if necessary.)

Section 2 – Description of Incident	
Description of the Incident:	(A clear, chronological account of what happened before, during, and after the incident e.g., fire, explosion, chemical spill, gas leak, power outage, violent attack, active shooter, terror attack, fatality, injury, epidemic, natural disaster, public health concern, cyber-attack, fraud, mismanagement, adverse behaviour, etc.)
Specific details:	(Actions taken, words spoken, and conditions e.g., weather, lighting.)
Injury or Damage Information:	(Details of any injuries sustained, including the type, severity, and part of the body affected.)
Injury or Damage Information:	(Description of any property damage that occurred.)
Immediate Actions Taken:	(First aid or emergency services provided.)



Measures taken:	<i>(I.e. to secure the area and mitigate further risks.)</i>
-----------------	--

Section 3: Witness Statements and Evidence	
Witness Statements:	<i>(Accounts from witnesses, including their perspective of how the incident occurred.)</i>
Contact information:	<i>(For each witness.)</i>
Photos:	<i>(Photographs of the scene, any hazards involved, and injuries or damages.)</i>
Supporting Documents:	<i>(Any relevant documents or materials, such as safety guidelines that were in place at the time.)</i>

Section 4: Impact Assessment	
Impact on Staff:	<i>(Describe any injuries, emotional distress, or other impacts on staff members.)</i>
Impact on Students:	<i>(Describe any injuries, emotional distress, or other impacts on students.)</i>
Impact on Visitors:	<i>(Describe any injuries, emotional distress, or other impacts on visitors.)</i>
Impact on Property:	<i>(Describe any damage to property or facilities.)</i>
Impact on Operations:	<i>(Describe any disruptions to Institute operations or activities.)</i>
Impact on Reputation:	<i>(Describe any potential or actual impact on the Institute's reputation.)</i>

Section 5: Outcome	
Analysis	<i>(Initial thoughts on contributing factors or causes of the incident.)</i>
Critical Incident Level	<input type="checkbox"/> Level 1 <input type="checkbox"/> Level 2 <input type="checkbox"/> Level 3
Actions	<i>(Any immediate corrective actions taken or proposed to prevent recurrence.)</i>
Follow-Up Actions	<i>(Details of further investigation required.)</i>
Future Planning	<i>(Planned corrective measures or changes to policies and procedures.)</i>

Section 6: Report Submission Information
--



Date	<i>(Date of report submission.)</i>
Signature	<i>(Of the person filling out the report, if required.)</i>
Confidentiality Statement (if applicable)	<i>(A note on the confidentiality of the information contained within the report, especially if sensitive or personal data is included.)</i>

Incident Classification and Escalation

The Institute uses a risk-based, critical incident classification and escalation process in alignment with the Institute's Risk Assessment Matrix to define the level of response required to manage incidents:

Level 1 (Minor) Incident

Has no more than a minor impact rating in any risk category and little or no potential to escalate.

- Can be resolved satisfactorily through standard procedures and channels.
- Can be managed satisfactorily at the local level by on-site personnel, which may include an Incident Management Team (IMT) if the incident is an emergency.

Level 2 (Moderate) Incident

Has no more than a moderate impact in any risk category but potential to escalate.

- May not necessarily be resolved satisfactorily by standard procedures and channels.
- Needs moderate levels of resource and input to manage, which may include a business continuity response and, if the incident is an emergency, an IMT.

Level 3 (Critical) Incident

Has a substantial, major, or catastrophic impact rating in any risk category and will be an event or issue that:

- Has a long-term or profound effect.
- Cannot be controlled through standard procedures and channels.
- Needs high levels of resources and inputs to manage, which will include the IMT and may include a Business Continuity response as directed by the Chief Executive Officer and Board of Directors.

Appendix 2: Accident Investigation Report Form

It is important to approach the situation with sensitivity and a focus on the welfare of the injured staff member, student, or visitor while also taking steps to prevent similar incidents in the future. Compliance with WHS legislation and continuous improvement of safety practices are essential for protecting all employees.

Ensure the accident investigation report is a comprehensive and detailed aids in understanding the sequence of events, identifying the root causes, and implementing effective preventative measures. It also serves as a legal document that can be crucial for insurance claims, regulatory compliance, and defending against potential lawsuits.	
Date and Time:	<i>(When the incident occurred.)</i>
Location:	<i>(Where the incident happened, with as much detail as possible.)</i>
Reporter's Details:	<i>(Name, position, and contact information of the person reporting the incident.)</i>
Involved Parties:	<i>(Names and roles of all individuals involved, including witnesses.)</i>
Contact information:	<i>(For those involved, if necessary.)</i>
Description of the Incident:	<i>(A clear, chronological account of what happened before, during, and after the incident.)</i>
Specific details:	<i>(Actions taken, words spoken, and conditions e.g., weather, lighting.)</i>
Injury or Damage Information:	<i>(Details of any injuries sustained, including the type, severity, and part of the body affected.)</i>
Injury or Damage Information:	<i>(Description of any property damage that occurred.)</i>
Immediate Actions Taken:	<i>(First aid or emergency services provided.)</i>
Measures taken:	<i>(I.e. to secure the area and mitigate further risks.)</i>
Witness Statements:	<i>(Accounts from witnesses, including their perspective of how the incident occurred.)</i>
Contact information:	<i>(For each witness.)</i>
Photos:	<i>(Photographs of the scene, any hazards involved, and injuries or damages.)</i>



Supporting Documents:	<i>(Any relevant documents or materials, such as safety guidelines that were in place at the time.)</i>
Analysis:	<i>(Initial thoughts on contributing factors or causes of the incident.)</i>
Actions:	<i>(Any immediate corrective actions taken or proposed to prevent recurrence.)</i>
Follow-Up Actions:	<i>(Details of further investigation required.)</i>
Future:	<i>(Planned corrective measures or changes to policies and procedures.)</i>
Report Submission Information:	<i>(Date of report submission.)</i>
Signature:	<i>(Of the person filling out the report, if required.)</i>
Confidentiality Statement (if applicable):	<i>(A note on the confidentiality of the information contained within the report, especially if sensitive or personal data is included.)</i>