Metavision Institute Pty Ltd
A.C.N 102 838 844

Critical Incident Policy

Purpose

This policy articulates Metavision Institute's management of critical incidents and ensures the interests of students; staff and their families are protected in the case of critical incidents. For international students, this policy is implemented in conjunction with Metavision Institute's obligations under the ESOS Act 2000 and the National Code 2018, ensuring that support and response actions align with their welfare and visa requirements.

Scope

This policy applies to all critical incidents that affect students, staff and visitors to Metavision Institute. Metavision Institute is committed to providing a positive and supportive environment for staff and students as a protective factor should critical incidents occur.

Relevant TEQSA Threshold Standards

This policy aligns with the requirements of sections:

Related HESF Domain	Section	Standard
Domain 2: Learning Environment	2.3	Wellbeing and Safety
Domain 6: Governance and Accountability	6.2	Corporate Monitoring and Accountability
Domain 7: Representation, Information and Information Management	7.3	Information Management

1. Policy

The following principles underpin this policy:

1.1 Metavision Institute prioritises the safety and well-being of its community and recognises its responsibility to prepare for and respond to critical incidents that may involve or impact its members.

1.2 Metavision Institute has comprehensive procedures in place for managing all stages of a critical incident, from initial response to recovery. Metavision Institute will maintain and regularly update detailed, incident-specific response protocols for a wide range of potential critical incidents.

1.3 Metavision Institute is committed to ensuring that the *Critical Incident Policy* and related procedures are accessible to individuals with diverse needs.

1.4 Metavision Institute prioritises the well-being of its students during and after critical incidents. The Institute will provide access to comprehensive support services, including mental health counselling, academic accommodations, and follow-up support, to ensure the holistic recovery of affected students.

1.5 Metavision Institute ensures that all international students are provided with readily accessible contact information for emergency services, medical care, and legal support services in Australia, to assist their adjustment to study and life in Australia, in compliance with National Code Standard 6.

1.6 Metavision Institute will establish and maintain clear, efficient, and multi-channel communication protocols for disseminating information during critical incidents. This will include the use of email, SMS alerts, website updates, social media, and other appropriate channels.

1.7 Metavision Institute ensures that all students and staff are fully aware of how to access the *Critical Incident Policy* and the procedures for reporting and seeking assistance, with this information made readily available during orientation, induction, and on the website.

1.8 Metavision Institute collaborates with external support services and relevant authorities to ensure a comprehensive response to critical incidents.

1.9 Metavision Institute provides regular training to staff and students on the *Critical Incident Policy*, including specific procedures for different types of incidents and available support services.

1.10 Metavision Institute will conduct regular testing and review of the *Critical Incident Response Plan* to ensure its effectiveness and identify areas for improvement. The plan will be reviewed annually, or more frequently as needed, to incorporate lessons learned and adapt to changing circumstances.

1.11 Metavision Institute maintains an emergency contact list with mobile phone numbers for key personnel, staff, emergency and health services, and relevant authorities.

1.12 Metavision Institute will conduct regular, formal risk assessments of all campus facilities and activities, utilising risk assessment matrices to identify, prioritise, and mitigate potential hazards, and will maintain a regularly reviewed and updated Risk Register to reflect the current risk profile.

1.13 Metavision Institute values the privacy of every individual and protects the personal information of all students and staff.

1.14 The *Critical Incident Policy* is regularly reviewed to ensure its continued effectiveness and alignment with best practices and regulatory requirements. Reviews involve consultation with staff, students, and external stakeholders.

1.15 Metavision Institute adheres to all reporting requirements regarding material changes, including critical incidents. Designated personnel are responsible for submitting timely notifications to TEQSA and other relevant authorities in accordance with established guidelines and timeframes.

2. Implementation

2.1 Initial Emergency Response:

2.1.1 In any situation posing an immediate threat to life or safety, students and staff must contact Emergency Services (000) immediately. This includes, but is not limited to:

2.1.1.1 Medical emergencies (e.g., heart attack, severe injury).

2.1.1.2 Fire or explosion.

2.1.1.3 Active shooter or violent intruder.

2.1.1.4 Immediate and credible bomb threats.

2.1.2 Following the call to Emergency Services, or concurrently, if possible, staff should notify the Chief Executive Officer (CEO) or designated on-call personnel.

2.2 Student and Staff Emergency Contact Information:

2.2.1 Students are required to provide and maintain up-to-date contact details, including emergency contact information, through the student portal or designated administrative channels.

2.2.2 Staff are required to provide and maintain up-to-date contact details and emergency contact information with Human Resources.

2.3 Critical Incident Definition and Types:

2.3.1 A critical incident is defined as any event that poses a significant threat to the safety, well-being, or operations of Metavision Institute. Examples include:

2.3.1.1 Medical Emergencies: Serious injuries, sudden illnesses, or fatalities.

2.3.1.2 Security Threats: Active shooter, bomb threats, violent intruders, cyberattacks.

2.3.1.3 Natural Disasters: Fires, floods, earthquakes, severe weather events.

2.3.1.4 Pandemics and Public Health Crises: Outbreaks of infectious diseases.

2.3.1.5 Mental Health Crises: Suicidal ideation, severe emotional distress.

2.3.1.6 Significant Infrastructure Failures: Loss of power, water, or internet access.

2.3.1.7 Major Accidents: Transportation accidents involving students or staff.

2.3.1.8 Reputational Crisis: Significant negative media coverage or public perception.

2.3.2 Responses will be tailored to the specific nature of the incident.

2.4 Critical Incident Response Team (CIRT):

2.4.1 The CEO is responsible for activating the CIRT upon notification of a critical incident.

2.4.2 The CIRT will consist of:

2.4.2.1 CEO: Overall command and control, media relations.

2.4.2.2 Dean: Student and staff welfare, academic continuity.

2.4.2.3 Facilities Manager: Building security, infrastructure, and safety.

2.4.2.4 Human Resources Manager: Staff support, emergency contact management.

2.4.2.5 IT Manager: Cybersecurity, communication systems.

2.4.2.6 Communications/Marketing Officer: Internal and external communications.

2.4.2.7 Designated First Aid Officers: Immediate medical assistance.

2.4.2.8 Student Support Services representative: student welfare and support.

2.4.3 CIRT responsibilities include:

2.4.3.1 Assessing the nature and severity of the incident.

2.4.3.2 Implementing appropriate response protocols.

2.4.3.3 Coordinating with emergency services.

2.4.3.4 Providing support to affected students and staff.

2.4.3.5 Communicating with stakeholders.

2.4.3.6 Documenting the incident and response.

2.4.3.7 Evaluating the effectiveness of the response.

2.4.4 Call escalation.

2.4.4.1 Incidents that require immediate police, fire or ambulance services are to be called directly by any staff or student that is aware of the incident. In addition to calling emergency services, those staff or students are to also inform the CEO or designated on-call personnel.

2.4.4.2 Incidents that do not require immediate emergency services, such as a student having a panic attack, are to be escalated to the student support services representative, or the Dean.

2.4.4.3 Incidents that involve potential legal or reputational damage are to be escalated to the CEO.

2.5 Incident-Specific Responses:

2.5.1 Bomb Threats:

2.5.1.1 Evacuate the affected area according to established evacuation procedures

2.5.1.2 Notify emergency services and the CEO immediately

2.5.1.3 Conduct a thorough search of the area if safe to do so

2.5.1.4 Do not touch suspicious packages

2.5.2 Active Shooter/Violent Intruder:

2.5.2.1 Implement "Run, Hide, Fight" protocols

2.5.2.2 Notify emergency services immediately

2.5.2.3 Secure the area and follow police instructions

2.5.3 Pandemics:

2.5.3.1 Implement public health guidelines (e.g., social distancing, hygiene protocols)

2.5.3.2 Transition to online learning or remote work as necessary

2.5.3.3 Provide regular updates to students and staff

2.5.3.4 Follow all government health orders

2.5.4 Medical Emergencies:

2.5.4.1 Provide immediate first aid if trained

2.5.4.2 Call emergency services

2.5.4.3 Notify the Dean or relevant staff

2.5.5 Cyberattacks:

2.5.5.1 Isolate affected systems

2.5.5.2 Notify the IT Manager and relevant authorities

2.5.5.3 Implement data recovery and security measures

2.6 Communication and Support:

2.6.1 The Chief Executive Officer (CEO) will be the designated spokesperson for Metavision Institute during critical incidents, ensuring consistent and accurate communication with media and external stakeholders, including media enquiries.

2.6.2 The CIRT will provide regular updates to students and staff through appropriate channels (e.g., email, website, social media).

2.6.3 Students and staff are encouraged to seek support from the Dean, CIRT members, or external counselling services.

2.6.4 The institute will provide sensitive and supportive communication to emergency contacts of affected individuals.

2.7 Business Continuity:

2.7.1 The Business Continuity Plan will be activated to ensure the continuation of essential operations.

2.7.2 This plan will include procedures for:

2.7.2.1 Remote work and learning

2.7.2.2 Data backup and recovery

2.7.2.3 Alternative communication systems

2.7.2.4 Maintaining essential services

2.7.3 The Business Continuity Plan will be regularly tested and updated.

2.8 Risk Management:

2.8.1 Critical incidents will be incorporated into the Institute's Risk Register.

2.8.2 Risk assessments will be conducted regularly, and mitigation strategies will be developed.

2.8.3 The Risk Register will be reviewed and updated to reflect changes in the risk profile.

2.9 Intensive vs. Normal Working Periods:

2.9.1 During intensive working periods, such as exam weeks, residential intensives, or conferences, the CIRT will ensure heightened vigilance and preparedness.

2.9.2 Emergency contact information for all participants will be readily available.

2.9.3 Evacuation and emergency procedures will be reviewed and communicated.

2.9.4 Designated on-call personnel will be identified and available.

3. Responsibilities

3.1 Corporate Board:

3.1.1 Approves changes to the Policy

3.1.2 Oversees policy implementation

3.2 Chief Executive Officer

3.2.1 Point of Contact for critical incidents; contactable via phone: +61 2 4862 2559

3.2.2 Ensure that Metavision Institute staff are familiar with this policy

3.2.3 Establish the Critical Incident Response Team

3.2.4 Allocate individual roles and responsibilities to members of the Critical Incident Response Team

3.2.5 Convene regular meetings of the Executive Committee to review incident scenarios and the Critical Incident Register, including actions taken, and to develop and document agreed protocols, including emergency contact details for key personnel, for engagement with external parties, including (but not limited to):

3.2.5.1 Emergency contacts for students and staff,

3.2.5.2 Police and other emergency services,

3.2.5.3 Hospitals and medical staff,

3.2.5.4 Relevant State and local Government authorities,

3.2.5.5 Professionally accredited and registered counsellors, and

3.2.5.6 Other groups as required.

3.2.6 Ensure that affected staff and students are supported.

3.2.7 Conduct a review of Metavision Institute's response to any critical incident.

3.2.8 Brief the Chair of the Governance Board about any critical incident as soon as it is contained.

3.2.9 Report critical incidents to TEQSA and other relevant authorities.

3.3 Critical Incident Response Team

3.3.1 Immediate Response:

3.3.1.1 Assess the Situation: Quickly gather information about the critical incident, including the nature of the event, the extent of the impact, and the individuals involved.

3.3.1.2 Ensure Safety: Take immediate action to ensure the safety and security of all individuals affected by the critical incident. This may include evacuation, lockdown, or providing first aid.

3.3.1.3 Activate Emergency Protocols: Implement the appropriate emergency protocols as outlined in the Critical Incident Policy and related procedures.

3.3.1.4 Communicate with Emergency Services: Contact and coordinate with emergency services, such as police, fire department, and ambulance, as required.

3.3.2 Advice and Assistance:

3.3.2.1 Provide Expert Advice: Offer expert advice to the Chief Executive Officer and other relevant stakeholders on the appropriate response to the critical incident.

3.3.2.2 Coordinate Support Services: Coordinate the provision of support services to individuals affected by the critical incident, including counselling, medical care, and academic support.

3.3.2.3 Liaise with External Agencies: Communicate and collaborate with external agencies, such as TEQSA, government authorities, and support organisations, as required.

3.3.2.4 Manage Communication: Develop and implement a communication plan to keep staff, students, and other stakeholders informed about the critical incident and the Institute's response.

3.3.3 Post-Incident Actions:

3.3.3.1 Conduct Debriefing: Conduct debriefing sessions for staff and students involved in the critical incident to provide support and gather feedback. In the event of a severe critical incident, Metavision Institute will consider engaging an external, qualified professional to conduct debriefing sessions, ensuring impartial support and expertise for staff and students.

3.3.3.2 Document the Incident: Ensure that the critical incident is properly documented, including the details of the event, the response actions taken, and the support services provided.

3.3.3.3 Review and Evaluate: Participate in the review and evaluation of the Institute's response to the critical incident to identify areas for improvement.

3.3.3.4 Contribute to Continuous Improvement: Contribute to the ongoing development and improvement of the Critical Incident Policy and related procedures.

3.3.4 Additional Responsibilities:

3.3.4.1 Maintain Confidentiality: Ensure the confidentiality of all information related to the critical incident and the individuals involved.

3.3.4.2 Act with Integrity: Uphold the highest standards of integrity and professionalism in all actions related to the critical incident.

3.3.4.3 Promote Wellbeing: Promote the wellbeing and safety of all members of the Metavision Institute community.

3.4 Executive Committee

3.4.1 Establish and maintain a structured incident review process

3.4.2 Develop and document comprehensive emergency protocols

3.4.3 Provide consistent and robust support to the CEO

3.5 Dean

3.5.1 Arrange debriefing of the affected students and for making referrals to external counsellors and psychotherapists.

3.6 Line Managers

3.6.1 Train new staff in this policy in their induction.

3.7 Finance, Audit and Risk Committee (FARC)

3.7.1 Monitors financial viability risks and cybersecurity risks as they relate to critical incident preparedness and institutional resilience, in accordance with the Business Continuity Plan.

3.7.2 Conducts quarterly compliance reviews to identify financial and operational risks that may affect the Institute's capacity to respond to critical incidents.

3.7.3 Receives and reviews significant or recurring LMS outage reports escalated by the IT Manager in accordance with the LMS and Learning Resources Procedure.

Definitions

Term	Definition
Emergency	A serious, unexpected, and often dangerous situation requiring immediate action.
Critical Incident	A Critical Incident means a traumatic event, or the threat of such (within or outside the campus), that is sudden, protracted, or ongoing, that causes high levels of stress, distress, fear, or injury, to students attending Metavision Institute, staff and/or visitors. Critical incidents are not limited to, but could include: ● A serious injury (for example, as a result of a traffic accident, violence, sexual assault, drug or alcohol abuse), ● An illness which has a seriously detrimental impact on a student's mental or physical health, ● A death, ● A missing student (neither staff nor any of the student's friends have been able to make any contact with the student for a period in excess of 24 hours), ● An act of terrorism,

	● Other events, such as a natural disaster, an infectious disease, a global financial crisis, or any other event that might impact on the health and safety of students and staff, ● Bullying, sexual harassment, sexual assault and theft.
Critical Incident Response Team	The Critical Incident Response Team means the group convened by the Chief Executive Officer for the purpose of providing immediate response, advice and assistance regarding Metavision Institute's response to critical incidents and associated impacts on its community.

Related Documents

Category	Documents
Policies	Anti-discrimination Policy
	Student Grievance, Complaints and Appeals Policy (Non-academic)
	Student Information and Communication Policy
	Student Welfare and Disability Policy
	Work Integrated Learning Policy
	Workplace Health and Safety Policy
	Privacy Policy
	Sexual Harassment and Sexual Assault Prevention Policy
Form	Critical Incident Report Form
Other	Business Continuity Plan
	Risk Management Framework
	Emergency Drill Schedule and Reporting
	Critical Incident Register
	Risk Register
	Critical Incident Protocol Suite
	Critical Incident Response Plan
	LMS and Learning Resources Procedure

METAVISION INSTITUTE
HOLISTIC EDUCATION

Version Control

Field	Detail
Document Title	Critical Incident Policy
Approved by	Governance Board
Version No.	v1.3; Reviewed: July 2026
Date approved	8 September 2026
Replaces Version No.	v1.2
Next review due	3 years from approval
Custodian	Chief Executive Officer