Institute of International Studies (IOIS)
ABN: 86636830263 RTO: 45883
Address: Suite 703, Level 7, 79 George Street
Parramatta, NSW-2150
https: www.iois.edu.au

Critical Incident Policy and Associated Procedures

Policy Area:	Student Safety, Welfare, and Emergency Management
Standards Reference:	Outcome Standard 1.6, 4.2 & Compliance Standard 20
Responsibility:	CEO, RTO Manager & All Staff
Classification:	Internal Governance and Safety Policy

1. Purpose

This policy outlines the approach of the **Institute of International Studies (IOIS)** to identifying, managing, responding to, and reviewing **critical incidents** that may impact students, staff, visitors, or the operation of the organisation.

The purpose of this policy is to ensure IOIS:

- Responds quickly and effectively to incidents that may affect the health, safety, or wellbeing of individuals,
- Minimises disruption to training operations,
- Meets its obligations under the Work Health and Safety Act 2011 (Cth) and Outcome Standards for RTOs 2025,
- Embeds incident response within the IOIS Risk Management and Self-Assurance Framework.

2. Scope

This This policy applies to all individuals, environments, and activities connected to IOIS operations. It ensures that critical incidents are managed consistently, regardless of where or how they occur.

- The policy covers every person who engages with IOIS in any capacity, including permanent staff, sessional trainers, external contractors, prospective and current students, guests, and any other individuals present in IOIS-controlled spaces. Each group may be involved in, witness, or be affected by a critical incident, and therefore must follow established procedures.
- Critical incidents can occur in physical IOIS campuses, third-party venues, work-placement sites, simulated learning environments, or digital platforms. This scope ensures consistent application of procedures across all learning modes—including virtual classrooms, online interactions, and any activities facilitated via IOIS technology systems.
- The policy applies to all IOIS-organised or endorsed events such as excursions, industry visits, practical placements, workshops, orientation sessions, student activities, and community events. Any activity arranged, supervised, or authorised by IOIS is included, regardless of whether it occurs on or off campus. This ensures that responsibilities and response protocols remain clear for all operational contexts.

3. Definitions

Term	Definition

Critical Incident	Any sudden or unexpected event causing or potentially causing significant harm to individuals or disruption to IOIS operations. Includes but is not limited to serious injury, death, fire, natural disaster, threats to personal safety, data breaches, and reputational harm.
Incident Coordinator	The person appointed by IOIS (typically the Academic Manager or WHS Officer) to manage the response and communication related to the incident.
Self-Assurance Review	A formal internal review process to evaluate IOIS's compliance and performance following an incident, identifying corrective and preventative actions.
WHS Representative	The designated officer responsible for health and safety compliance and reporting.

4. Policy Statements

IOIS takes all reasonable steps to prevent, prepare for, and respond to critical incidents.

IOIS is committed to creating a safe and supportive learning environment by actively identifying potential risks, implementing preventative strategies, and ensuring readiness to respond to incidents that may threaten the health, safety, or wellbeing of students, staff, or visitors. This includes maintaining up-to-date emergency procedures, staff training, and access to appropriate resources and support services.

A Critical Incident Management System (CIMS) is maintained to ensure timely and coordinated responses.

IOIS operates a structured Critical Incident Management System that outlines clear roles, responsibilities, communication protocols, and escalation pathways. The system ensures that responses to incidents are immediate, coordinated, and effective. It includes procedures for identifying incidents, activating emergency response processes, engaging relevant internal and external authorities, and ensuring accurate, timely communication with all affected parties.

IOIS provides appropriate support to those affected, including emotional, academic, and operational support.

Following a critical incident, IOIS ensures affected individuals receive tailored support, which may include psychological first aid, counselling referrals, academic extensions or adjustments, and practical assistance (e.g., safety considerations, access to resources, or relocation of training activities). IOIS recognises that different individuals may experience incidents differently and commits to offering compassionate, flexible, and culturally sensitive support.

All incidents are recorded, reported, and reviewed to identify lessons learned and support continuous improvement.

Every critical incident must be documented using the IOIS Critical Incident Form and entered into the relevant registers. Incident reports must capture key details including the nature of the incident, individuals involved, actions taken, and outcomes. IOIS will conduct post-incident reviews to analyse the effectiveness of the response, identify contributing factors, and determine strategies to prevent recurrence. Findings are used to strengthen organisational systems, emergency preparedness, and risk management frameworks.

Information relating to incidents will be handled confidentially and in accordance with IOIS's Privacy Policy.

IOIS is committed to protecting the privacy and dignity of individuals involved in critical incidents. All records, discussions, and communications will be handled sensitively, securely, and in line with legislative privacy obligations. Information will only be shared with authorised personnel on a need-to-know basis, or where required by law or emergency services.

The CEO is responsible for ensuring that corrective actions are implemented and that systemic risks are managed through the Risk Register and Continuous Improvement Register (CIR).

The CEO oversees organisational follow-up after each critical incident to ensure all recommended actions are completed within appropriate timeframes. This includes updating risk ratings, implementing changes to prevent future incidents, allocating resources where required, and ensuring improvements are captured in IOIS's Continuous Improvement Register. The CEO ensures that lessons learnt from incidents inform policy updates, staff training, and strategic planning.

5. Procedures

5.1 Prevention and Preparedness

- Each year, IOIS undertakes a structured review of all operational areas—including classrooms, offices, online systems, training sites, and external event locations—to identify conditions or practices that may lead to critical incidents. This assessment considers physical risks (e.g., fire, equipment failure, medical emergencies), behavioural risks (e.g., violence, harassment), environmental risks (e.g., extreme weather, power outages), and technological risks (e.g., system failures, cybersecurity issues).
- Findings are documented in the IOIS Risk Register, with assigned responsibilities and timelines to ensure preventative controls are implemented. High-risk items are prioritised for immediate action to minimise the likelihood of escalation into a critical incident.
- IOIS ensures all learners, visitors, and staff are familiar with emergency responses by providing clear, accessible signage and instructions throughout all campuses. Evacuation maps, assembly points, first-aid resources, and emergency contact details are displayed in classrooms, corridors, and common areas. During student orientation and staff induction, IOIS explains emergency procedures, evacuation routes, lockdown protocols, and expected behaviours during emergencies. This ensures individuals know how to respond quickly and safely should an incident occur.
- Every new staff member—including trainers, administrators, and contractors—receives a comprehensive safety induction that outlines:
  – how to recognise and respond to critical incidents
  – who to contact in an emergency and how to escalate concerns
  – how to complete incident reports and notify relevant IOIS personnel
  – their role in supporting students and minimising harm
  – obligations under the Critical Incident Management System (CIMS)
- Staff are expected to maintain awareness of updates to safety procedures and participate in refresher briefings as required. By ensuring all staff understand their roles, IOIS strengthens its capacity to prevent incidents and respond swiftly and effectively when they occur.

5.2 Immediate Response

- Ensure Safety and Contain Risk
  - **Provide first aid where possible and contact local emergency services immediately by dialling *000* in Australia.**
    Staff trained in first aid must respond promptly, ensuring injured individuals receive urgent care while awaiting emergency services. The responding staff member must remain with the affected person (if safe) until help arrives.
    Where first aid capability on-site is limited, staff must focus on maintaining safety and preventing further harm while emergency services are deployed.
  - **Evacuate affected areas if necessary.**
    If there is a threat to safety—such as fire, chemical spill, structural damage, gas leak, or violent behaviour—staff must initiate evacuation following the campus emergency plan. Evacuation must be orderly, prioritising vulnerable individuals and ensuring everyone proceeds to the designated assembly point.
  - **Isolate hazards or restrict access until safe.**
    Where dangers remain present (e.g., damaged equipment, unsecured area, biological hazard), staff must close off the area and prevent entry. No person should re-enter until the area has been formally assessed and declared safe by emergency services or authorised IOIS personnel. Containment helps prevent escalation and protects bystanders from harm.

- Notify Key Personnel
  - The first staff member on scene must notify the **Incident Coordinator** (Academic Manager or CEO).

    This initial notification triggers IOIS's Critical Incident Management System (CIMS). The staff member must provide clear details, including location, nature of the incident, individuals involved, and the actions already taken.
  - The Incident Coordinator determines if the situation qualifies as a *critical incident* and activates the response plan.

    If the event poses, or has the potential to pose, serious harm to individuals or disrupt IOIS operations, it must be classified as a critical incident. The coordinator then mobilises relevant personnel, enacts communication protocols, and ensures continuity and control of the situation.
- Incident Coordination
  - The Incident Coordinator ensures communication with emergency services, staff, and affected individuals.

    This includes relaying essential information, assigning responsibilities, directing staff support, and ensuring emergency services receive accurate situational updates. Internal communications must be coordinated to avoid confusion or duplication.
  - All actions are recorded in the Critical Incident Register.

    Records must include:
    - incident details
    - timeline of events
    - actions taken
    - personnel involved
    - communication logs
    - follow-up requirements

    Documenting each action supports legal compliance, WHS reporting obligations, future investigation, and continuous improvement.
  - If the incident involves injury, WHS reporting obligations are triggered and the incident must be reported to SafeWork NSW if notifiable.
- Communication Management
  - The CEO or delegated representative is the **official spokesperson** for all external communications.
  - IOIS ensures that information is accurate, timely, and protects the privacy and dignity of those involved.

5.3 Support for Affected Persons

IOIS provides or facilitates:

- IOIS ensures that individuals receive immediate medical attention following an incident. This includes providing on-site first aid, arranging transport to medical facilities, or coordinating with emergency responders. Staff remain with the affected individual (where appropriate) to offer assistance, reassurance, and continuous monitoring until medical professionals take over.
- Critical incidents can cause emotional distress, trauma, or ongoing psychological impact. IOIS facilitates access to professional mental health services, including crisis helplines, counselling providers, or community wellbeing organisations. The Student Support Officer ensures individuals are informed of available options and assists with referrals where consent is provided.
- Students affected by a critical incident may require flexibility to support their academic recovery. IOIS may implement:
  - extensions for assessment tasks
  - temporary modifications to study load
  - alternative training arrangements
  - deferment or leave options where necessary

These adjustments aim to ensure students are not academically disadvantaged due to circumstances beyond their control.

- Where a student or staff member experiences a significant incident, IOIS may assist in notifying their nominated emergency contacts, provided this is appropriate, lawful, and in the individual's best interest. IOIS ensures communication is handled sensitively, respectfully, and with regard to privacy requirements.
- Where ongoing support is required, the Student Support Officer coordinates and monitors the individual's wellbeing, academic adjustments, and any follow-up actions. This includes:
  - checking progress after the incident
  - ensuring support measures remain appropriate
  - updating relevant staff where required (on a need-to-know basis)
  - scheduling additional meetings if circumstances change

The overarching objective is to ensure that individuals affected by the incident receive continuous, meaningful support and are not disadvantaged—academically, emotionally, or operationally—during their recovery.

5.4 Investigation and Documentation

- The Incident Coordinator ensures completion of an **Incident Report Form** within **24 hours** of the event.

  Immediately following the stabilisation of the incident, the Incident Coordinator is responsible for ensuring that a comprehensive Incident Report Form is completed. This documentation must capture:
  - a precise description of what occurred
  - individuals involved or affected
  - timelines and sequence of events
  - immediate actions taken and by whom

  Completing the report within 24 hours ensures the information remains accurate, detailed, and reliable for subsequent review and compliance reporting.
- Evidence, photos, or witness statements (if applicable) are attached to the report.

Supporting evidence strengthens the accuracy and integrity of the incident review. This may include:

- photographs of the scene or hazards
- CCTV footage (if available)
- written witness accounts
- copies of emails, logs, or communications relevant to the incident

Such documentation assists IOIS in determining root causes, validating the actions taken, and mitigating future risks. All evidence is stored securely in accordance with privacy and recordkeeping requirements.

- A formal review is undertaken by the CEO and Academic Manager to determine:
  - Contributing factors,
  - Preventive actions,
  - Policy or procedure changes required.
- Findings are recorded in the Continuous Improvement Register (CIR) and the Risk Register if the incident exposed systemic weaknesses.

5.5 Post-Incident Review and Self-Assurance

- Within **10 working days** of the incident, IOIS conducts a **post-incident review meeting** involving relevant staff.
- The review assesses:
  - Adequacy of the immediate response,

- Communication effectiveness,
- Compliance with IOIS procedures,
- Training gaps or resource deficiencies.

- The CEO ensures corrective actions are implemented and monitored.
- Lessons learned feed into the annual Self-Assurance Review, informing policy updates, PD plans, and risk management strategies.

5.6 Recordkeeping

- All records (incident forms, investigation reports, correspondence, and follow-up actions) are stored securely in IOIS's central compliance system.
- Records are retained for at least **seven years**.
- Sensitive information is restricted to authorised personnel and handled per the IOIS Privacy Policy.

6. Responsibilities

Role	Responsibilities
CEO	Approves and oversees the critical incident response and ensures regulatory reporting compliance.
Academic Manager / Incident Coordinator	Leads immediate response, manages communication, coordinates reviews, and ensures follow-up support.
Trainers / Staff	Report incidents promptly, assist in managing safety, and complete incident documentation.
Student Support Officer	Provides welfare support, referrals, and ongoing follow-up for affected students.
WHS Officer	Ensures SafeWork notifications are completed (if required) and that corrective actions are implemented.

7. Related Documents

- IOIS Risk Management Policy
- IOIS Privacy Policy
- IOIS Student Support Policy
- IOIS Health and Safety Policy
- IOIS Continuous Improvement Register
- Incident Report Form and Critical Incident Register

Institute of International Studies (IOIS)
ABN: 86636830263 RTO: 45883
Address: Suite 703, Level 7, 79 George Street
Parramatta, NSW-2150
https: www.iois.edu.au

Document Version Control

Document Title	IOIS Critical Incident Policy and Associated Procedures
Reviewed By	Compliance Manager
Approved By	Chief Executive Officer

Version	Changelog	Created / Modified Date
1.0	IOIS Critical Incident Policy and Associated Procedures *V1.0*	July 2025