ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

Critical Incident and Emergency Management Policy and Procedure

Approving body	Governing Board (GB)
Date approved	17 August 2026
Date of effect	Commencement of operation
Next scheduled review	Two years from when policy commence
Policy owner	Chief Executive Officer
Policy contact	Chief Executive Officer
Related Documents	Business Continuity Plan Health and Safety Policy and Procedure OHS Strategy Quality Assurance Framework Records and Data Management Policy and Procedure Risk Management Framework Sexual Harm Prevention and Response Policy and Procedure Student Wellbeing Policy and Procedure Student Support Framework Risk Register
Related Legislative and Regulatory Instruments	HESF Standard 2.3.5 HESF Standard 6.2.1 HESF Standard 7.3.3 Australian Qualifications Framework (AQF) Tertiary Education Quality and Standards Agency Act 2011 (TEQSA Act) Education Services for Overseas Students Act 2000 (ESOS Act)

ZENITH INNOVATION INSTITUTE
UNPARALLELED EXCELLENCE

Immediate response to incidents or hazards

- If there is a risk to life, always call 000.
- Students should report incidents or hazards promptly to Student Services in person, via email (XXX), or by phone (XX XXXX XXXX).
- Staff should report incidents or hazards to their line manager in person, via email, or by phone.
- The incident site should not be interfered with unless safe to do so and only to assist injured persons at risk of further harm, to make the area safe, or as directed by emergency services.
- Staff informed of an incident should inform a member of the Critical Incident Team (CIT) as soon as possible and record key details in a Critical Incident Report (see Appendix 1).
- All available members of CIT should convene immediately to assess the incident.

Emergency contact numbers:

Campus Emergency: +61 x xxxx xxxx

Police, Fire, Ambulance: 000

Purpose

1. The purpose of this Policy and Procedure is to plan for, respond to and manage critical incidents that may impact **Zenith Innovation Institute's** (**Zenith / ZII / the Institute**) and members of the Zenith community.
2. An incident is considered critical (refer Schedule 1 for detailed examples) if the incident requires immediate attention and decisive action to:
   (a) prevent / minimise any negative impact on the health and welfare of members of the Zenith community
   (b) mitigate any on Zenith assets and operations and
   (c) protect Zenith's reputation.
3. This Policy and Procedure is intended to enable Zenith to return to business-as-usual operations as soon as possible following a critical incident.
4. This Policy and Procedure is also designed to meet the requirements mandated by the *Higher Education Standards Framework (Threshold Standards) 2021* (**HESF**) and other regulatory and legislative instruments.

Scope

5. This Policy and Procedure applies to all incidents that have impacted or have the potential to impact on Zenith community, services and operations, property and the environment. This includes physical actions or hazards and incidents that may disrupt its operations and/or cause major reputational damage to Zenith (refer Schedule 1).

   This Policy and Procedure applies to all staff, students, members of governing bodies, contractors and consultants and all Institute campuses, sites operated by third-party providers or third-party sites which are the location for study tours or work integrated learning.

Policy

6. There is a risk that Zenith may be vulnerable to a range of critical incidents and emergencies that occur. The Institute will develop and implement systems for appropriate and effective management of these situations.

7. This Policy and Procedure outlines protocols for the management of critical incidents and emergencies and provides information about appropriate resources.

8. Zenith will comply with all reporting requirements including, but not limited to: privacy requirements, crime and corruption, environmental and health, ethical conduct, obligations to students and insurance requirements.

Principles

Emergency planning and management

9. Zenith will establish a Critical Incident Team (CIT) led by the CEO, comprising key staff members, including representatives from Student Services, Academic Affairs, Facilities Management, and Human Resources. The CIT membership list will be publicly available to staff and students, with regular updates communicated through internal channels, including the staff/student handbooks. The CIT will ensure that site-specific emergency plans and procedures are maintained, implemented, and communicated regularly.

10. Each member of the Critical Incident Team has defined domain responsibilities in both the response and recovery phases:

    (a) Chief Executive Officer (CIT Lead) — overall coordination of the incident response; external communications with TEQSA, media, and regulatory bodies; activation of the Business Continuity Plan; escalation to the Governing Board; and sign-off on all material decisions relating to the incident response;

    (b) Academic Dean (Academic Continuity Lead) — management of academic continuity for currently enrolled students, including alternative delivery arrangements, assessment extensions or deferrals, and communication with teaching staff about adjustments to the academic program;

    (c) Student Services Manager (Student Welfare Lead) — communication with affected students; referral to emergency support services; management of student welfare needs during and after the incident; and liaison with the Overseas Students Ombudsman and TPS Administrator where international students are affected; and

    (d) IT/LMS Support Officer (Infrastructure Lead) — management of ICT systems and facility-related aspects of the incident; coordination of physical access to Institute premises; and implementation of IT-related business continuity measures including LMS backup arrangements.

Incident risk assessment

11. Any incident or emergency that occurs will be evaluated as soon as possible to assess its severity and determine an appropriate response. A designated CIT member will assess the incident based on the Risk Management Framework, in consultation with relevant stakeholders, including Student Services and the reporting party. Incident responses will be scalable, depending on the nature and severity of the incident. Where an incident concerns the health and safety of a staff member, contractor, student or visitor, including a Work-Integrated Learning (WIL) placement site, the CIT member will also assess and respond in accordance with the OHS Strategy.

12. Incidents that are not deemed to be critical will be managed as part of business-as-usual processes.

13. The Business Continuity Plan will be activated for significant incidents that disrupt normal operations, ensuring a structured recovery process.

14. To ensure continuous improvement and risk mitigation, the Risk Management Framework, Risk Register, and Student Support Framework will be utilised in evaluating responses and implementing corrective actions. The Governing Board and Audit Risk Committee will oversee risk assessments and ensure self-assurance measures are in place.

15. The Student Support Framework will be referenced to provide appropriate support to students directly or indirectly affected by an incident, including onlookers. Similarly, support will be offered to staff involved in any incidents.

Incident management

16. All critical incidents and emergencies will be managed by the CIT unless it is deemed that an alternative management approach is more appropriate.

17. The CEO or a nominated member of CIT will mobilise the required resources.

18. Following the completion of a response to a critical incident, a review will be undertaken to determine the effectiveness of the response and any improvements that can be made going forward.

19. Where the Chief Executive Officer is unavailable, directly affected by, or has a conflict of interest in relation to the incident, the Academic Dean assumes the role of Acting CIT Lead for the duration of the CEO's unavailability. The Acting CIT Lead notifies the Governing Board Chair within two hours of assuming the role, and the Governing Board Chair may convene an emergency Governing Board meeting within 24 hours if the nature of the incident warrants Board-level oversight.

International students

20. The *Education Services for Overseas Students Act 2000* (**ESOS Act**) sets out the legal framework governing delivery of education to international students in Australia on a student visa. In relation to this Policy and Procedure specifically, Zenith will comply with Standards 6.8-6.9 of the *National Code of Practice for Providers of Education and Training to Overseas Students 2018*.

Off-campus considerations

21. Zenith's Executive Management Team is responsible for ensuring there is consistency with Zenith policies and procedures and for reviewing incident and emergency policies and procedures when Zenith enters into agreements with third-party providers and when there are material changes.

22. Students and staff involved in an incident occurring at a third-party provider or third-party site are to follow the third-party provider's incident management procedures.

23. In the event of an off-campus incident, an Incident Report is required to be submitted to Zenith's CEO.

Recording and reporting

24. The CEO or a nominated member of CIT is responsible for ensuring that:

    (a) Incident Reports are completed and maintained in accordance with Zenith's *Records and Data Management Policy and Procedure* and reported to the Governing Board (GB) and

    (b) any external reporting obligations required by legislation are met.

25. Reporting Process:

- Students must report incidents to the Student Support Officer (SSO).
- Staff must report incidents to their line manager.
- The receiving officer will escalate the matter to the CIT if deemed a critical incident based on the Risk Management Framework.
- All reported incidents, whether critical or non-critical, will be recorded in the Incident Register, which will be regularly reviewed as part of the Risk Register and Risk Management Framework

Reporting a critical incident

26. Students should report incidents or hazards promptly to Student Services in person, via email (xxxx), or on the phone (XX XXXX XXXX).

27. Staff should report incidents or hazards to their line manager in person, via email, or on the phone.

28. Student Services or the relevant line manager should inform a CIT member, who will assume immediate responsibility for controlling the situation.

Managing a critical incident

29. The CIT member will:

(a) attend the incident

(b) offer immediate assistance to persons involved

(c) inform the CEO, who will assess the situation, consider any risks to those present and inform other members of the CIT as required

30. Upon a critical incident being declared, the full Critical Incident Team convenes within two hours of the declaration. The initial CIT meeting assesses the immediate safety and welfare of students, staff, and visitors; activates domain-specific response actions; determines the communication strategy for students, staff, and external stakeholders; and establishes a schedule for subsequent CIT meetings during the recovery phase.

(a) contact and liaising with Emergency Services as required and

(b) document details of the incident.

31. Upon managing the critical incident, the CIT member will:

(a) notify the emergency contacts for students or staff involved in the incident and providing appropriate support. If an international student dies or sustains serious injury, support may include assisting family members by completing necessary tasks on their behalf in Australia

(b) coordinate appropriate psychology, counselling and/or support services for any student who was harmed and/or assaulted and/or harassed

(c) coordinate appropriate counselling and support services for any students involved or any students requiring assistance and support

(d) manage internal and external communications.

32. The CIT will organise ongoing response/follow up (including staff briefing, counselling, review and reporting) as part of the process.

Recording and reviewing a critical incident

33. After the critical incident has been managed and resolved, a CIT member must complete a Critical Incident Report (an example is provided at Schedule 2) containing the following details:

    (a) Type of critical incident

    (b) Exact location of the critical incident

    (c) Details of person(s) involved in the critical incident and who may be injured, or in distress and in need of counselling, or at risk. If current students are affected, a copy of the student's Written Agreement[1] (adapted for domestic students) should accompany the Critical Incident Report.

34. The Critical Incident Report will be used to:

    (a) review the situation and identify future priorities

    (b) ensure compliance with any relevant legislative requirements associated with the incident and

    (c) coordinate communications to the Zenith community, families and the media if required

    (d) communicate with TEQSA and the Department of Home Affairs, as required, and in the case of a student's death or absence affecting the student's course progression, report through the *Provider Registration and International Student Management System* (PRISMS).

35. A de-briefing session will be organised by the CIT to evaluate the effectiveness of the critical response procedures and inform the preparation of a report to the GB which will include recommendations for managing future critical incidents, if necessary.

36. Ongoing support will be provided to ensure there is follow-up with those involved in the incident.

Accountabilities

37. The GB is responsible for:

    (a) the wellbeing and safety of students, staff and visitors to Zenith

    (b) monitoring the occurrence and nature of critical incidents and that action is taken to address underlying causes (HESF Standard 6.2.1j).

    (c) managing and mitigating risks to Zenith in accordance with its Risk Management Framework and Risk Register

38. The CEO or a nominated member from the CIT will:

    (a) be available during hours of operation in case of incidents or emergencies

    (b) manage the processes for preventing, preparing for, responding to, and recovering from critical incidents

    (c) ensure staff are trained to respond to critical incidents

    (d) ensure that appropriate information is provided to students

    (e) ensure that a network of services is maintained to respond to different types of incidents including counselling services, police, hospitals and legal centres.

[1] National Code Standard 3

39. The Chief Executive Officer reports annually to the Governing Board on the Institute's critical incident preparedness, including any incidents that occurred in the preceding year, the effectiveness of the Critical Incident Team response, and any improvements made to the critical incident management process. The Governing Board reviews this report and approves any amendments to the critical incident management framework required to maintain HESF compliance.

40. The CIT will manage critical incidents and emergencies until normal operations can resume.

Definitions

41. For the purposes of this Policy and Procedure, the following terms are defined as follows:

Term	Definition
Campus	Any campus or site owned or operated by Zenith.
Institute community	Institute students, staff, and other stakeholders engaging with Zenith, including visitors, contractors and volunteers.
Critical Incident	The National Code defines a 'critical incident' as: A traumatic event, or the threat of such (within or outside Australia), which causes extreme stress, fear or injury.
Emergency	A sudden, unexpected event that requires an immediate response from internal and external emergency services.
Incident	An issue or occurrence that requires a response but is not critical, has a localised containable impact and unlikely to escalate in severity. The required response and management will be part of ongoing business-as-usual.
Third-party providers	Organisations contracted by Zenith to provide services on its behalf.
Third-party sites	Sites that Zenith staff or students visit other than Institute campuses and third-party providers' premises. This includes sites where staff and students may be on work placements or study tours.

Version History

Version	Changes	Approval Body	Approval Date
1.0	New Policy	Governing Board (GB)	21 Mar 2024
1.1	Added "Risk Register; Student Support Framework" under Related documents Under Related Legislative and Regulatory Instruments added "Australian	GB	27 Feb 2025

Version		Changes	Approval Body	Approval Date
		Qualifications Framework (AQF) Tertiary Education Quality and Standards Agency Act 2011 (TEQSA Act) Education Services for Overseas Students Act 2000 (ESOS Act)" Point 9 Replaced "Zenith will establish a Critical Incident Team (**CIT**) led by the CEO, which will ensure that site-specific plans and procedures are maintained and implemented. These plans and procedures will be comprehensive, consistent and communicated to staff and students regularly." Point 10 replaced "Any incident or emergency that occurs is to be evaluated as soon as possible to assess its severity and determine an appropriate response. Incident responses will be scalable depending on the nature and severity of the incident." Added Point 13, 14, 15 and 23		
1.2	Added Critical Incident Team Domain Responsibilities and Convening Protocol section per HESF 6.2.1(e): defined domain responsibilities for CEO (coordination), Academic Dean (academic continuity), Student Services Manager (student welfare), and IT/LMS Support Officer (infrastructure); CEO unavailability escalation protocol (Academic Dean as Acting CIT Lead, GB Chair notified within 2 hours); 2-hour CIT convening timeframe; and annual	Added Critical Incident Team Domain Responsibilities and Convening Protocol section per HESF 6.2.1(e): defined domain responsibilities for CEO (coordination), Academic Dean (academic continuity), Student Services Manager (student welfare), and IT/LMS Support Officer (infrastructure); CEO unavailability escalation protocol (Academic Dean as Acting CIT Lead, GB Chair notified within 2 hours); 2-hour CIT convening timeframe; and annual	GB	

Version		Changes	Approval Body	Approval Date
	Governing Board self-assurance review.	Governing Board self-assurance review.		
1.3		Restructured V1.2 orphaned “Critical Incident Team Domain Responsibilities and Convening Protocol” section. Content integrated into policy body: CIT domain responsibilities (CEO/Academic Dean/Student Services Manager/IT-LMS Support Officer) integrated into Emergency planning and management section; CEO unavailability escalation protocol (Academic Dean as Acting CIT Lead, GB Chair notified within 2 hours) integrated into Incident management section; 2-hour CIT convening timeframe integrated into Managing a critical incident procedure; self-assurance reporting obligation added as concluding paragraph in Accountabilities section. ‘IT and Facilities Officer’ corrected to ‘IT/LMS Support Officer’ and ‘Executive Management Committee’ corrected to ‘Executive Management Team (EMT)’ throughout, consistent with Delegations Policy and Schedule. Duplicate V1.2 version control text removed. HESF citation headings and prescriptive language removed.	Governing Board	
1.4		Added 'OHS Strategy' to Related Documents. Point 11 (Incident risk assessment) updated to specify that incidents concerning the health and safety of staff, contractors, students or visitors (including at WIL placement sites) are also assessed and responded to	Governing Board	17 August 2026

Version	Changes	Approval Body	Approval Date
	in accordance with the OHS Strategy, in response to TEQSA Statement of Reasons para. 29e.		

Schedule 1 – Examples of critical incidents

The National Code[2] defines a 'critical incident' as: A traumatic event, or the threat of such (within or outside Australia), which causes extreme stress, fear or injury.

Critical incidents may include, but are not limited to:

- serious injury, illness, or death of a student or staff member
- students or staff members lost or injured during fieldwork experiences
- a missing student
- severe verbal or psychological aggression
- physical assault
- student or staff members witnessing a serious accident or incidence of violence
- natural disaster e.g. epidemic, earthquake, flood, windstorm, hailstorm, or extremes of temperature
- traumatic incident within an international student's home country, such as a political coup, religious persecution, natural disaster
- fire, bomb-threat, explosion, gas or chemical hazard or
- social issues e.g. sexual assault, drug use, alcohol abuse, internet abuse.

An incident is considered critical if the incident requires immediate attention and decisive action to:

- prevent / minimise any negative impact on the health and welfare of members of the Institute community
- mitigate any of the Institute's assets and operations
- protect the Institute's reputation.

[2] National Code 2018 Standard 6

Schedule 2 – Critical Incident Initial Report

Date of Incident	
Reported by	
Description of Incident	
What happened?	
Location of the incident	
Time and date of the incident	
Lists the people involved	
Who did the incident affect	
Who was notified about the incident	
Other relevant information	
Lists supporting document and attach clearly labelled	

Name:

Signature:

STAFF USE ONLY

Report Reference Number:

Received on:

Acknowledged on:

Passed to responsible officer (Critical Incident Team (CIT) member):