

Critical Incident Management and Business Continuity Procedure

1. Contents

1. Contents.....	2
2. Preamble.....	3
3. Purpose.....	3
4. Scope.....	3
5. Definitions.....	3
6. Procedure.....	3
7. Referred Legislation and References.....	8
8. Relevant HEA Policies and Procedures.....	8
9. Document and Version Details.....	9
10. Procedure Inquiries.....	9

2. Preamble

The framework for critical incident management is based upon planning and preparedness for the four prime responses following any critical incident:

- i. Emergency response: providing capability to manage the immediate issues arising from an incident and focusing on protection of life and property;
- ii. Business continuity – providing capability for the continuation of critical business operations;
- iii. Recovery: restoring crucial business operations and infrastructure to a state of routine operation; and
- iv. Evaluation and critical review.

This procedure aligns with the *Higher Education Standards Framework (Threshold Standards) 2021*, the *National Code of Practice for Providers of Education and Training to Overseas Students 2018*, the *Work, Health and Safety Act*, the *Emergency Management Act 2013 (Vic)*.

3. Purpose

This procedure provides the process to identify and effectively manage critical incidents. It provides the process to sustain critical business operations and then transition to normal operations and critically evaluate the institute's response.

4. Scope

The procedure applies to all staff at HEA involved in responding to and managing critical incidents affecting HEA. This includes contractors and third parties engaged by HEA where relevant to incident response.

5. Definitions

Please refer to the Glossary of Terms.

6. Procedure

6.1 Planning and Preparedness

6.1.1 The following documents are accessible to all staff to ensure the institute's readiness and preparedness for responding to critical incidents:

- a) Critical Incident Management Plan;
- b) Business Continuity Plan;
- c) Guidelines for Pandemics;
- d) IT Disaster Recovery Plan;
- e) Emergency Management Procedure; and
- f) Risk Management Plan.

These documents are approved, maintained and reviewed in accordance with HEA governance and risk management arrangements.

6.1.2 Staff are provided comprehensive training in relation to critical incidents and business continuity and made aware of the location of all relevant documents relating to critical incidents.

6.2 Identifying and Reporting a Critical Incident

6.2.1 Any staff member who first encounters a critical incident will assume responsibility for the institute's initial response by assessing the situation to determine if there is an immediate risk to the safety or health of any person.

6.2.2 If the incident is potentially dangerous or life threatening or a person is injured, emergency services (police, ambulance or fire) must be contacted immediately on triple zero (000).

6.2.3 Staff must follow the Critical Incident Management Plan which forms part of the Risk Management Plan.

6.2.4 As soon as practicable, the staff member is also required to complete a Critical Incident Response Report and provide it to the Dean or CEO. Material incidents will be escalated through HEA's governance and risk management processes.

6.2.5 The relevant staff member must complete the Critical Incident Response Checklist.

6.2.6 The Critical Incident Response Report must include:

- a) A summary of the type of critical incident;
- b) A summary of events;
- c) A copy of the completed Critical Incident Response Checklist;
- d) A list of all persons involved and their role; and
- e) The current outcome of the incident and the ongoing activity in response to the incident.

6.2.7 Critical incident information is disclosed only to those who have the right to the information by virtue of their role in the management process or as required by law.

6.3 Responding to a Critical Incident

- 6.3.1 A critical incident may warrant the formation of a critical incident response team. The Dean or CEO (or relevant nominee) will make this decision based on the immediate assessment and availability of senior staff members, taking into consideration if incident has occurred outside of usual business hours.
- 6.3.2 To adequately contain and respond to the critical incident, a critical incident response team may be required to implement one of the following plans, available on the staff intranet:
- a) Emergency Management Plan;
 - b) Psychological First Aid Plan; or
 - c) Incident Action Plan (for fire, storm, evacuation, lock down or shelter, medical emergency, personal safety, cyber security).
- 6.3.3 If emergency services are required to attend the incident, all staff and students comply with instructions and directions of emergency services.
- 6.3.4 If evacuation is required, a designated staff member will accompany students during the evacuation process and remain outside in the designated area until the incident is resolved.
- 6.3.5 Following the immediate responses to the incident, a secondary round of responses must be taken by the critical incident response team, or Dean, CEO (or relevant nominee):
- a) Liaising with emergency services personnel;
 - b) Ensuring any physical injuries have been treated by emergency services personnel;
 - c) Ensuring any psychological injuries have been treated or referred for treatment by emergency services personnel or counsellors;
 - d) Contacting family members or emergency contacts if required; and
 - e) Directing the safe and secure resumption of critical operations if possible.
- 6.3.6 If the critical incident involves a death, the CEO, Dean or relevant nominee will contact the deceased's family to offer support.
- 6.3.7 If the incident involves an overseas student's death, critical injury or suicide, the student's family will be informed and the necessary assistance provided. Actions may include the following:
- CEO, Dean or relevant nominee contact the overseas student's next of kin and/or emergency contact;
 - Accredited interpreters may be hired to interpret or translate for the family;
 - Assist in making travel arrangements and temporary accommodation for the family if necessary;
 - Support staff, counselling staff, legal services and religious representatives may be engaged;
 - Assist in making funeral arrangements, repatriation, rehabilitation and memorial services where necessary;
 - Obtain a death certificate and other necessary documentation;
 - Assist with the dispatch of personal belongings and managing personal affairs that may include liaising with health insurers on behalf of the overseas student's family;
 - Communicate with the Department of Home Affairs in regard to the death of a visa holder;

- The incident will be documented and immediately reported through the *Provider Registration and International Student Management System (PRISMS)*;
- Counselling services will be arranged for students and staff not directly involved in the incident;
- Maintain accurate records throughout the process; and
- Send condolences to everyone involved.

6.4 Recovering from Critical incidents

- 6.4.1 The critical incident response team will design and direct a comprehensive recovery process aligned with the Business Continuity Plan included in the Risk Management Plan after the immediate aspects of the critical incident are under control, to address short term resumption of critical activities or operations. Recovery actions and decisions will be documented.
- 6.4.2 The Dean, CEO or relevant nominee will delegate responsibility for the resumption of critical activities or operations to the relevant staff members and specify any alternative arrangements in consideration of the impact of the critical incident.
- 6.4.3 Resumption of normal operations and activities must occur as soon as practicable, taking into account the nature of the critical incident and its impact upon stakeholders.
- 6.4.4 The Dean, CEO or relevant nominee will direct the institute as a whole to resume normal activities and operations, with any necessary alterations.

6.5 Evaluation and Critical Review

- 6.5.1 Following the occurrence of a critical incident and resumption of normal business activities, the CEO, Dean or relevant nominee will establish a critical incident review team to evaluate the following:
- Whether the critical incident risk was correctly categorised in relation to its likelihood and impact;
 - The appropriateness of the initial response;
 - The depth and accuracy of the Critical Incident Response Report;
 - The appropriateness of the actions required to resume critical operations and activities;
 - The appropriateness of the institute's resumption of normal operations and activities; and
 - Whether this procedure should be amended to better respond to critical incidents and ensure business continuity.
- 6.5.2 The CEO, Dean and Board of Directors will analyse the findings of the critical incident review team and take any steps necessary to improve the institute's response to critical incidents.
- 6.5.3 Annual critical incident management cycles are coordinated by the Audit and Risk Management Committee and comprises:
- Identification of the key risks that pose a threat to the institute and that contribute to critical incidents;
 - Ensuring all emergency response plans and resources are in place;
 - Confirming the responsibilities of the emergency response team;
 - Conducting a Business Impact Analysis (BIA) covering the key business functions of the institute;
 - Reviewing, updating and maintaining the Business Continuity Plan covering the critical business functions of the institute; and

- An annual review of its plans. The Audit and Risk Management Committee will report to the Board of Directors and provide recommendations for improved safety and risk management. They will also identify to the board if any changes need to be made to the Business Continuity Plan.

6.6 Delegation and Responsibility

The Board of Directors has delegated responsibility for this procedure to the Chief Executive Officer.

6.7 Review and Improvement

- 6.7.1 Updates to this procedure can be made at any time to ensure the implementation of the Critical Incident Management and Business Continuity Policy.
- 6.7.2 The Board of Directors will ensure an internal review of this procedure is conducted at least once every two years and will ensure that any improvements identified from the review are implemented, including updates to the procedure itself.
- 6.7.3 The Board of Directors will engage external reviewers at least once every seven years to conduct a review of this procedure and will ensure that recommended improvements are actioned.
- 6.7.4 At their own discretion, the Board of Directors may undertake a review of this procedure as needed.

6.8 Feedback

Feedback, including recommended improvements, is welcomed in relation to this procedure.

7. Referred Legislation and References

AS 3745-2010 Australian Standard – Planning for emergencies in facilities

<https://www.fireserviceprofessionals.com.au/images/stories/PDFs/qld-building-fire-safety-regulation-2008/3745-2010.pdf>

Best Practices in Business Continuity Planning for Higher Education (2020, updated 2022)

by Tanecia Jackson <https://www.azeusconvene.com/articles/best-practices-in-business-continuity-planning-for-higher-education>

Education Services for Overseas Students (ESOS) Act

<https://www.legislation.gov.au/Details/F2019L00993>

Emergency Management and Security Services Support – Victoria State Government – education and training

Guide to Occupational Health and Safety Regulations 2017

<https://www.worksafe.vic.gov.au/resources/guide-occupational-health-and-safety-regulations-2017>

Higher Education Standards Framework (Threshold Standards) 2021

<https://www.teqsa.gov.au/higher-education-standards-framework-2021>

ISO31000 – International Standards for Risk Management <https://www.iso.org/iso-31000-risk-management.html>

National Code of Practice for Providers of Education and Training to overseas students:

Standard 6: Student Support Services <https://www.dese.gov.au/esos-framework/national-code-practice-providers-education-and-training-overseas-students-2018>

Occupational Health and Safety Regulations 2018 <https://www.legislation.vic.gov.au/in-force/statutory-rules/occupational-health-and-safety-regulations-2017/012>

State Emergency Management Plan Cyber Security Sub-Plan Edition 2

<https://www.emv.vic.gov.au/responsibilities/semv-sub-plans/state-emergency-management-plan-cyber-security-sub-plan-edition-2>

TEQSA Guidance Note – Wellbeing and Safety -

<https://www.teqsa.gov.au/latest-news/publications/guidance-note-wellbeing-and-safety>

Victorian Guide to occupational Health and Safety (updated 2022)

<https://www.nfplaw.org.au/free-resources/work-health-and-safety-laws/victoria>

8. Relevant HEA Policies and Procedures

- Acceptable Use of Resources Policy
- Acceptable Use of Resources Procedure
- Business Plan
- Enrolment Variation Policy
- Health and Safety Policy
- Health and Safety Procedure
- Infrastructure and Resources Policy
- Infrastructure and Resources Procedure
- Records and Information Management Policy
- Records and Information Management Procedure
- Risk Management Policy
- Risk Management Procedure
- Student Academic Progression Policy
- Student Academic Progression Procedure
- Student Wellbeing and Support Policy
- Student Wellbeing and Support Procedure
- Teach Out Policy

9. Document and Version Details

Approval Authority	Board of Directors
Approval Date	4 March 2026
Review Date	4 March 2029
Version	5.0

10. Procedure Inquiries

For any inquiries about this procedure, please email us. (admin@heau.edu.au)