Critical Incident Policy

Purpose/objective

This Critical Incident Policy sets out AAHE's commitment and approach to managing critical incidents safely and effectively. The Policy is designed to:

a) protect AAHE employees, students, associates, and other stakeholders such as partners, neighbours and visitors to the campus
b) protect AAHE's assets and environment
c) ensure continuity of AAHE's critical business activities, and
d) protect AAHE's public reputation.

Scope

This Policy applies to the management of any critical incident that has an impact on the AAHE community or activities. It extends to all administrative units, staff and affiliates, students, visitors and contractors engaged with or controlled by AAHE.

Definitions

Business continuity	The capability of the organisation to continue service delivery at acceptable predefined levels following a disruptive incident.
Critical Incident	A traumatic event, or the threat of such (within or outside Australia) which causes extreme stress, fear or injury and has the potential to threaten AAHE's assets, operations, environment, and requires urgent attention.
Critical Incident Management Plan	A critical incident procedure that describes AAHE's incident management arrangements.
Critical Incident Response Team	The team responsible for providing executive decisions and strategic direction on AAHE's priorities when responding to critical incidents.
Response time objective (RTO)	The RTO is the time from which disruption occurs to the time the business function must be operational in order to avoid serious harm to students and/or financial loss to the business.

Policy

1 A critical incident is defined by the ESOS National Code (Standard 6) as "a traumatic event, or the threat of such (within or outside Australia) which causes extreme stress, fear or injury"[1]. The incident may be a single event or series of events that is sudden, overwhelming, threatening or protracted. The incident may endanger physical safety through assault, threat, severe injury, fire, flood or electrocution. Not all critical incidents are corporeal in nature, however, but can include such traumatic events as major fraud, breaches of cybersecurity or public humiliation.

2 AAHE's approach to critical incident management follows the 'Prevention, Preparedness, Response and Recovery (PPRR) framework developed by Business Queensland[2]. The Critical Incident Policy and Procedure focuses primarily on the third, **Response**, stage of the model. The initial, **Prevention**, stage is the subject of AAHE's Risk Management Plan, and stages two, (**Preparedness**) and four (**Recovery**) are covered in our Business Continuity Plan.

3 AAHE uses the following risk-based critical incident classification and escalation process.

A Level 1 (minor) incident is a local event or issue that:

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

b) can be resolved satisfactorily through standard procedures and channels

c) can be managed satisfactorily at the local level by on-site personnel, which may include a member of the Critical Incident Response Team if necessary.

[1] https://internationaleducation.gov.au/regulatory-information/Education-Services-for-Overseas-Students-ESOS-Legislative-Framework/National-Code/nationalcodepartd/Pages/ExplanatoryguideD6.aspx
[2] https://www.publications.qld.gov.au/dataset/business-continuity-planning-template/resource/63f7d2dc-0f40-4abb-b75f-7e6acfeae8f3

A Level 2 (moderate) incident is an event or issue that:

a) has no more than a moderate impact in any risk category but the potential to escalate

b) may not necessarily be resolved satisfactorily by standard procedures and channels

c) needs moderate levels of resource and input to manage, which may include a business continuity response and, if the incident is an emergency, the Critical Incident Response Team.

A Level 3 (critical) incident is substantial, major or catastrophic event that:

a) has a long-term or profound effect

b) cannot be controlled through standard procedures and channels

c) needs high levels of resources and inputs assigned to the Critical Incident Response Team.

4 AAHE's Executive Management Committee will constitute the Critical Incident Response Team, and will be chaired by the Chief Executive Officer. When the critical incident is IT related, the LMS/IT Manager will also be a member of the Critical Incident Response Team. The role of the Critical Incident Response Team is to oversee AAHE's emergency management, which involves:

a) Emergency management planning and preparation
b) Training
c) Review and compliance.

5 AAHE will maintain a Critical Incident Procedure and a trained and competent Critical Incident Response Team to control AAHE's strategic response and provide executive decisions and strategic direction relating to a critical incident.

6 AAHE will undertake an annual internal review of the Critical Incident Procedure and complete annual training and testing of AAHE's Critical Incident Response Team and associated systems and capabilities.

Responsibilities

7 All staff, students and users of AAHE's services and systems have a responsibility to:

a) Minimise the risk of physical harm to self and others
b) Report suspected or actual critical incidents promptly so that appropriate action can be taken to minimise harm
c) Minimise the risk of vital or confidential operations being lost or falling into the hands of people who do not have the right to see or use them
d) Protect the security and integrity of AAHE's IT systems on which vital or confidential information is stored or processed.

8 The Executive Management Committee is responsible for the strategic direction, development, implementation, management and validation of capabilities and functions to manage critical incidents, specifically:

a) The Chief Executive Officer is AAHE's Critical Incident Coordinator and is responsible for adequately resourcing the critical incident management program.
b) The Chief Operating Officer is responsible for the health, wellbeing and safety procedures relating to staff including local emergency arrangements.

c) The Dean is responsible for the health, wellbeing and safety procedures relating to students.
d) The Marketing Manager is responsible for incident management and emergency procedures relating to members of the AAHE community overseas.
e) The LMS/IT Manager is responsible for Information Technology (IT) incident management procedures.

Related documents and relevant legislation

Higher Education Standards Framework (Threshold Standards) 2021
TEQSA Guidance Note: Wellbeing and Safety
National Code of Practice for Providers of Education and Training to Overseas Students 2018
Risk Management Policy and Plan
Information Technology Services Policy and Procedures
Business Continuity Policy, Procedure and Plan
Prevention of Fraud Policy and Procedure
Health and Safety Policy and Procedure

Document information

Document owner: Board of Directors

Version	Approved by	Approved on	Implementation date	Changes made
1	Board of Directors	14/10/21	1/10/23	

Critical Incident Procedure

AAHE's critical incident response begins with the classification by the most senior staff member on site of the incident's level of urgency according to *Critical Incident Policy*. This decision will be consistent with policy and the incident's Response Time Objective (see *Business Continuity Plan* for further detail).

1. Detecting and reporting a critical incident

Any incident has the potential to start as or escalate into a critical incident. All incidents must be reported to the most senior staff member available if the incident:

a) cannot be controlled through standard procedures; or

b) threatens or has potential to threaten the AAHE community or AAHE's operations, assets or environment.

2. Responding to a critical incident

2.1 **Physical danger**

2.1.1 All incidents reported to staff are classified as Level 1, 2 or 3 according to the risk-based critical incident classifications outlined above. Other than fire, which is handled according to AAHE's fire response procedures, Level 2 or 3 incidents will be communicated to the most senior contactable member of the Critical Incident Response Team who will confirm the classification and, where necessary, notify emergency services before notifying the Chair and the Board of Directors of any incident that is classified as Level 2 or 3 and activating the Critical Incident Response Team. Where appropriate the Critical Incident Response Team Leader (the CEO) will then consult one or more of the following:

a) Emergency services once the immediate crisis has passed

b) relevant government agencies such as the Commonwealth Department of Health and the Victorian Department of Health and Human Services

c) travel warnings issued through the government *SmartTraveller* website[3] or AAHE's approved Travel Consultant

d) relevant international agencies such as the World Health Organisation

e) AAHE business units to determine the impact of the incident on the AAHE community and/or activities.

2.1.2 The Critical Incident Response Team will make all necessary executive decisions and provide strategic direction on AAHE priorities when responding to the incident. In arriving at their decisions, the Critical Incident Response Team may need to:

a) seek advice from legal counsel about any statutory obligations or external reporting obligations arising from the critical incident

b) ensure that stakeholders and regulatory bodies, including but not limited to, the Tertiary Education Quality Standards Agency, WorkSafe Victoria and AAHE's insurer are notified in a timely manner and provided with appropriate information.

[3] https://www.smartraveller.gov.au/

2.1.3 Subject matter experts within AAHE may be enlisted by the Critical Incident Response Team to:

a) assist with the response

b) implement any operational guidelines relating to a specific incident type, e.g. international student incidents, off-shore incidents or international crises.

2.1.4 AAHE carries comprehensive insurance against critical incidents. Where applicable, uninsured costs incurred by a student or student's next of kin or family as a result of a critical incident will be met by the student or the student's family, unless:

a) Approval to provide ex gratia financial support has been granted by the Chief Executive Officer; or

b) AAHE legal counsel determines that AAHE has an obligation to provide financial support.

2.2 Fraud

2.2.1 The definition and prevention of fraud is the subject of AAHE's *Prevention of Fraud and Misconduct Policy and Procedure*. The reporting procedures presented here are replicated in that document along with the key definitions, scope and objectives of fraud prevention at AAHE. The reader is therefore referred to the *Prevention of Fraud and Misconduct Policy and Procedure* for a more comprehensive overview of AAHE's approach to fraud and its management.

2.2.2 AAHE must ensure that all staff are aware of fraud reporting procedures and actively encourage all staff to report suspected cases of fraud through the appropriate channels. Staff who become aware of suspected fraudulent conduct are required to report the matter in accordance with this procedure. Staff are also required to maintain strict confidentiality on any suspected fraud matter about which they have knowledge.

2.2.3 In the first instance, the issue should be reported to the person authorised by the Board of Directors to receive whistleblower disclosures. If, for any reason, the staff member considers that reporting the incident through this channel would be inappropriate, he or she may report the matter directly to the Chief Executive Officer or, if it involves the CEO, to the Chair of the Board. Such reports may be made confidentially, if desired.

2.2.4 AAHE strives to meet or exceed best practice standards on whistleblower protection under the 2018 amendments to the Corporations Act (2001). The amendments greatly strengthened the standards that apply to commercial operations like AAHE and are intended to ensure that AAHE:

a) requires staff to act in good faith and reasonably in making reports under whistleblower protection

b) recognises and respects the confidentiality of the identity of a *bona fide* informant

c) provides support and protection to an informant against any form of recrimination or reprisal or any threat of detriment.

2.2.5 Further information on the rights and protection of whistleblowers can be found on the Australian Securities and Investment Commission (ASIC) website[4,5]. Among those protections

[4] https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/whistleblower-rights-and-protections/

[5] https://asic.gov.au/about-asic/asic-investigations-and-enforcement/whistleblowing/protections-for-corporate-sector-whistleblowers/

is the provision that civil *and* criminal penalties can apply to individuals authorised to receive whistleblower allegations "for causing or threatening detriment to (or victimising) a whistleblower and for breaching a whistleblower's confidentiality" (ASIC Fact Sheet, 2019)[5].

2.2.6 Fraud investigation will follow principles of natural justice. AAHE will appoint individual(s) who are impartial and who possess appropriate expertise to conduct the investigation. Following internal investigation, the matter may be reported to the police for further action or investigation.

2.2.7 The investigator(s) will consider all relevant legislative or regulatory obligations (see above) in assessing, investigating, managing and reporting matters of alleged fraud.

2.2.8 In each instance where fraud is investigated, AAHE will reassess the adequacy of the internal control environment particularly those controls directly relevant to the fraud incident and provide a written report to AAHE's Audit, Risk and Finance Committee (ARF) on the implementation of any improvements. Where improvements are necessary, they will be implemented as soon as practicable under the supervision of ARF.

2.2.9 AAHE will actively pursue the recovery of any money or property lost through fraud after considering all relevant issues.

2.2.10 Any fraud risks identified during the fraud risk assessment, and any action taken by AAHE will be collected, classified and reported to the relevant authorities, having regard to privacy, confidentiality, legal professional privilege and the requirements of natural justice.

2.3 **Information technology-related incidents**

2.3.1 IT Critical Incident Management is a structured approach, composed of four steps:

1) Detection and analysis
2) Containment and eradication
3) Communication and engagement
4) Recovery.

The procedures that apply at each of these stages are set out in AAHE's Cyber Incident Response Plan.

3. Communication protocol

In the case of critical incidents, the following communication protocol applies:

1. The CEO will make decisions on the appropriate communications protocol to be adopted.
2. The CEO will nominate one person to be the authorised spokesperson for any matter.
3. Any communication by a person other than the CEO or authorised person is forbidden.

4. Recovering from a critical incident

4.1 The Critical Incident Response Team will design and implement a comprehensive recovery process when the immediate aspects of a critical incident are under control, addressing short and long term issues. When an incident disrupts a critical activity or process, AAHE's *Business Continuity Plan* will be implemented. AAHE undertakes a process of learning and adapting after critical incidents through debriefs conducted before the Critical Incident Response Team is stood down.

4.2 After the debriefing and evaluation program is complete, the Critical Incident Response Team oversees a comprehensive follow-up process designed to:

a) provide proper closure for those involved in an incident, and

b) enable AAHE to identify lessons learned and implement improvements that reduce vulnerabilities to similar situations in the future.

5. Record keeping

The Dean will ensure that a written record of any critical incident and remedial action taken is kept on an affected student's file for at least 2 years after the student ceases to be an accepted student.

Document information

Document owner: Principal and Chief Executive Officer

Version	Approved by	Approved on	Implementation date	Changes made
1	Board of Directors	14/10/21	1/10/23	