

Critical Incident Policy

1. Purpose and Scope

- 1.1 The Critical Incident Policy outlines AIAT's response to a Critical Incident during and in the period immediately following an incident. It should be read in conjunction with the Critical Incident Procedure.
- 1.2 This policy applies to all AIAT staff and students.
- 1.3 This policy does not apply to
 - 1.3.1 local Critical Incident management arrangements applying to third party organisations that may be involved in the delivery of AIAT's courses (e.g. placement providers). AIAT will satisfy itself that third parties have appropriate and effective incident management policies and procedures in place.
 - 1.3.2 Information technology systems failures and disaster recovery.

2. Definitions

Refer to Glossary of Terms for commonly used terms. The definitions below are included for clarity.

Critical Incident - refers to a traumatic event, or the threat of such (within or outside Australia), which causes extreme stress, fear or injury. It can include (but it not limited to): natural disasters; death; serious injury; attempted suicide; arrest or detainment of a student or staff member; robbery; missing students; bomb-threats; riots; toxic/chemical release or explosions; pandemics and epidemics; deprivation of liberty; sexual assault; kidnapping or attempted kidnapping; violence; or severe verbal or psychological aggression. It includes a matter deemed by the CEO to be dealt with as a Critical Incident under this Policy.

3. Policy Statement

- 3.1 AIAT is committed to providing a safe environment for students and staff and minimising the impact that a disruptive incident can have on individuals and its business functions. It recognises that incidents can arise that have the potential to impact seriously on the safety of staff, students or visitors to AIAT and/or AIAT's business continuity and has a Business Continuity Plan in place to provide guidance.
- 3.2 AIAT is committed to ensuring its response to a Critical Incident is managed effectively, compassionately, in a timely manner, and that appropriate resources are made available to respond to all aspects of the Critical Incident.
- 3.3 AIAT is committed to complying with its reporting and notification requirements in the event of any breaches of relevant legislation, standards or guidelines. This includes but is not limited to privacy requirements, crime and corruption, environmental and health,

ethical conduct and student obligations. AIAT will also comply with its obligations from an insurance reporting perspective.

4. Policy Principles

- 4.1 AIAT aims to ensure that appropriate resources are available to respond to all aspects of a Critical Incident, including:
 - 4.1.1 physical and psychological safety of affected students and staff;
 - 4.1.2 emotional and physical support; and
 - 4.1.3 interventions required at different phases following an incident.
- 4.2 Responses to Critical Incidents will be timely and professional, and take into account the safety of individuals involved as the paramount consideration.
- 4.3 Where it is suspected that a crime has taken place, care shall be taken to preserve the scene of the incident and any related evidentiary items, provided that it is feasible to do so without adversely impacting on health and safety.
- 4.4 AIAT will keep appropriate records of Critical Incidents which have occurred and the follow up action taken.

5. Roles and responsibilities

- 5.1 The Campus Manager
 - 5.1.1 is the first point of contact when a Critical Incident occurs;
 - 5.1.2 manages the Critical Incident response;
 - 5.1.3 updates and maintains the Critical Incident Register;
 - 5.1.4 provides regular reports to the Student Welfare and Services Committee regarding Critical Incidents which involve students; and
 - 5.1.5 provides annual reports to the Executive Management Group on the types of incidents that have occurred, how they were managed and recommended improvements.
- 5.2 The CEO will advise the Board of Directors of Critical Incidents classified as Moderate or Major and any actions that have been taken once the event is under control.

6. Policy Details

Institution	Australian Institute of Advanced Technologies (AIAT)
Policy name	Critical Incident Policy
Policy Reference No.	POL – 07
Policy Approval	Board of Directors
Policy Authority	Executive Management Group
Responsible Officer	CEO
Governance Reference	HESF 2021: 2.3.5

Threshold Standards	
Related Documents	Critical Incident Procedure Health and Safety Policy Privacy Policy Risk Management Policy Risk Management Register
Related Legislation	Commonwealth Education Services for Overseas Students Act 2000 (ESOS) Higher Education Standards Framework (Threshold Standards) 2021 (HESF) National Code of Practice for Providers of Education and Training to Overseas Students 2018
References	AIAT has referred and benchmarked with the following institutions and policies during the creation of this policy: Alphacrucis College (2021) Critical Incident Management Policy Deakin University (unknown) Critical Incident Management Policy, <i>retrieved 9 Dec 2021</i> James Cook University (2018) Incident Management Policy Kaplan (2021) Critical Incident Policy Southern Cross University (unknown) Student Critical Incident Management Policy, <i>retrieved 9 Dec 2021</i> The University of Adelaide (2018) Student Critical Incidents Policy The University of Notre Dame (2019) Policy: Critical Incident Management University of the Sunshine Coast (2020) Critical Incident Management – Governing Policy
Date of approval	3 February 2022
Review date	December 2024
Policy Category	Governance

6. Document Version Control

Document No	POL – 07	Last Modify Date	Summary of Changes
Version No	1.0	NA	Initial version approved by Board of Directors
	1.01	8/3/2022	Fixed typo
Created Date	Feb 2022		