

CRITICAL INCIDENT POLICY

Purpose

To outline AIB's approach to respond to and manage critical incidents affecting students and staff.

Scope

This policy applies to all students and staff of Australian Institute of Business (AIB). As AIB has a documented Business Continuity Plan, this policy does not apply to disaster recovery processes for the organisation but rather applies to situations where the welfare and safety of an individual or groups of people is threatened or affected.

Definitions

Unless otherwise defined in this document, all capitalised terms are defined in the [glossary](#).

1. Policy

AIB is committed to ensuring the safety and wellbeing of its students and staff. A Risk Management Plan has been established in which the organisation implements its plans to proactively prevent incidents which may have a detrimental impact as much as possible. Plans and actions are regularly reviewed and updated. The AIB Risk Register is a mechanism for ensuring key risks are identified, addressed and reviewed.

However, there are occasions where unforeseeable incidents may occur at specific locations and/or that occur to individual persons.

- The AIB webpage '[Student Safety and Wellbeing](#)' is provided to communicate how students can report critical incidents, and to promote awareness of the various support services provided by AIB and also by the broader community during and post-incident.
- Information for staff regarding safety and wellbeing is provided in the AIB Staff Handbook, as available on the staff-access-only Employment Hero portal and Intranet. Staff should immediately report Critical Incidents within the workplace directly to the Critical Incident Team Leader.
- The Critical Incident Policy and internal procedures documentation, as part of AIB's Risk Management Plan, is designed to guide the organisation to implement actions within appropriate timeframes to manage such critical incidents.

2. Critical Incident Team

The (internal) Critical Incident Procedure provides guidance on the response AIB will take where a critical incident occurs including the formation of a Critical Incident Response Team. The Critical Incident Team Leader (CITL) is the Finance Director.

The Critical Incident Team is a team that the CITL may assemble as required and which may include members of the leadership team, First Aid Officers and other staff as required and as appropriate to the nature of the critical incident.

3. Principles

- This policy has been developed to reflect Australian Institute of Business (AIB)'s commitment in providing a safe environment for students and staff.
- AIB recognises the duty of care owed to its students and staff and that planning for the management of a Critical Incident is essential.
- AIB 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.
- AIB will ensure staff and students have appropriate information to report Critical Incidents as they occur, and will provide reasonable support for staff and students and, where appropriate, their families who may be affected by a Critical Incident.
- This policy enables AIB to have clear decision-making processes for managing and reporting on student Critical Incidents to ensure that each case is managed effectively, consistently, compassionately, and expeditiously.

Responsibility:

Chief Executive Officer

Related Policies and Procedures:

Critical Incident Procedure (internal)

[Sexual Assault and Sexual Harassment Policy](#)

[Sexual Assault and Sexual Harassment Procedure](#)

[Support for Students Policy](#)

[Support for Students Procedure](#)

Related Resources:

Business Continuity Plan (internal)

Risk Management Plan (internal)

Staff Handbook (internal)

[Student Safety and Wellbeing webpage](#) on the AIB website

Related Legislation:

Higher Education Support Act 2003

Higher Education Provider Guidelines 2022

Higher Education Standards Framework (Threshold Standards) 2021

Current Status:	Version 7.1
Approved By:	Board of Directors
Date of Approval:	4 April 2024
Effective From:	4 April 2024
Previous Versions:	10 February 2022 4 June 2020 31 January 2019 24 November 2016 12 August 2015 1 July 2011 5 November 2010 25 February 2010
Date of Next Review:	10 February 2025