THE UNIVERSITY OF NOTRE DAME AUSTRALIA

Policy:

Critical Incident Management

Effective: 19 April 2023

Audience: Staff and Students

Policy Category: Governance
Policy Sub-category: Health, Safety and Wellbeing

Key words:	critical incident, critical incident officer
Policy Owner:	Deputy Vice Chancellor, Finance & Chief Operating Officer
Responsible Officer:	Chief Property and Facilities Officer
Review Date:	December 2025

Contents

1. OBJECTS OF THE UNIVERSITY

The University's Objects are defined in Section 5 of its Act of Parliament:

The Objects of the University are:

(a) the provision of university education, within a context of Catholic faith and values; and

(b) the provision of an excellent standard of -

i. teaching, scholarship and research;

ii. training for the professions; and

iii. pastoral care for its students.

2. PURPOSE

2.1. The Policy: Critical Incident Management (**Policy**) outlines the University's response to a Critical Incident during and in the period immediately following an incident and for management of the longer-term consequence of such an incident.

3. SCOPE

3.1. This Policy applies to all areas of the University.

3.2. Critical Incidents may occur on a University Campus or site, or elsewhere and includes or involves without limitation:

3.2.1. A Student, Staff member or Visitor in the course of attendance at the University;

3.2.2. A Student, Staff member or Visitor's participation in officially sanctioned University activities (including non-academic activities);

3.2.3. A Staff member (including contractors) in the course of their duties on behalf of the University; and/or

3.2.4. Serious damage, or incidents with a potential for serious damage or harm, to University property located at a University Campus or site (this includes major cyber and IT security incidents e.g., hacking, ransomware etc.).

3.2.5. In relation to overseas students, a traumatic event, or the threat of such (within or outside Australia), which causes extreme stress, fear or injury that could affect a student's ability to undertake or compete their program.

3.3. This Policy does not apply to:

3.3.1. Local Critical Incident management arrangements applying at third party organisations that may be involved in the delivery of the University's Programs;

3.3.2. Non major cyber or IT security information technology systems failures and disaster recovery; refer to the *Information Technology Disaster Recovery Plan*; or

3.3.3. Business continuity procedures – refer to the *Business Continuity Plan*.

4. PRINCIPLES

The University recognises that each incident will be unique and is committed to ensuring that each incident is managed effectively, compassionately and with the safety and welfare of all concerned being of priority.

4.1. The University 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 and support of affected Students, Staff and Visitors;

4.1.2. Protection and security of University property; and

4.1.3. Interventions required at different phases following an incident.

4.2. The University will keep appropriate records of Critical Incidents occurring and follow up action taken.

4.2.1. In relation to overseas students, the Director of Student Engagement and Support will maintain a written record of any critical incident and remedial action taken for at least two years after the overseas student ceases to be an accepted student under the ESOS Act.

4.3. Responses to Critical Incidents will be timely and professional and consider the safety of individuals involved as the paramount consideration.

4.4. 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, if it is feasible to do so without adversely impacting on health and safety.

4.5. The level of response required to a Critical Incident may vary in accordance with the circumstances and scale of the Critical Incident. The *Procedure: Critical Incident Management* sets out the University's considered response to a Critical Incident. It is not to be viewed as restricting any response by the **Incident Controller** or the **Critical Incident Management Team**.

5. ROLES AND RESPONSIBILITIES

5.1. The Policy places responsibility on all Staff across the University.

5.2. **All Staff** must be aware of this Policy and all procedures for managing a Critical Incident, and in particular the contact details for Security and Emergency Services.

5.3. A **Staff** member involved in, witnessing or becoming aware of or, suspecting a Critical Incident will have immediate responsibility for responding to the situation, where appropriate, and contacting **Security** (for campus, student or staff-related incidents) or the **Notre Dame IT Service Desk** (for cyber-related incidents).

5.4. For campus, student or staff-related incidents, where appropriate, **Security** (or by agreement the staff member, student or visitor) must contact the relevant Emergency Services, the University **Logistics, Security & Facilities Officer** and the **Incident Controller.**

5.5. For cyber-related incidents, the Notre Dame IT Service Desk will update the **Director, IT Business Partners & Security** of the incident. The Director, IT Business Partners & Security must inform the **Incident Controller**.

5.6. The **Incident Controller** (**IC**) is responsible for:

5.6.1. Confirming the incident is to be dealt with as a Critical Incident under this Policy;

5.6.2. Communicating this to the Deputy Vice Chancellor, Finance & Chief Operating Officer or Vice Chancellor as soon as reasonable; and

5.6.3. Convening the Critical Incident Management Team (**CIMT**) as required.

5.7. The **IC** has responsibility for controlling the situation and liaising with relevant subject matter experts. The IC is to ensure pertinent details of the incident (i.e. impacted parties, situational developments) are reported to the CIMT.

5.8. **Members of the CIMT** have responsibility for the response and recovery of an incident, including:

5.8.1. Coordination of Emergency Evacuation Procedures (if required).

5.8.2. Ensuring effective ongoing management of the incident and post recovery.

5.8.3. Notifying relevant emergency contacts for Staff or Students involved in the incident and providing appropriate support.

5.8.4. Coordinating appropriate counselling and support services.

5.8.5. Managing internal and external communications, including with regulators where required.

5.8.6. Completing a confidential Critical Incident Occurrence Report to the Deputy Vice Chancellor, Finance & Chief Operating Officer and Vice Chancellor.

5.8.7. Implementing an ongoing plan of support to ensure follow up concerning the well-being of individuals involved in the incident.

5.8.8. Ensuring (in conjunction with the Legal Office and other relevant subject matter experts) that the University complies with any additional legislative reporting requirements that may arise from the incident.

5.8.9. Making recommendations for the management of such incidents in the future.

5.9. The **Incident Controller** has responsibility for the training of the CIMT and any improvement actions identified from post-incident reviews.

5.10. The **Deputy Vice Chancellor, Finance & Chief Operating Officer** has the responsibility for the update and management of the **Critical Incident Management Policy** and **Procedure**.

6. RELATED DOCUMENTS

6.1. *Education Services for Overseas Students (ESOS) Act 2000*
6.2. *National Code of Practice for Providers of Education and Training to Overseas Students 2018*
6.3. *Work Health and Safety Act 2020 (WA)*
6.4. *Work Health and Safety Act 2011 No 10 (NSW)*
6.5. *Code of Conduct: Students*
6.6. *Employee Code of Conduct and Ethical Behaviour*
6.7. *Procedure: Critical Incident Management*
6.8. *Procedure: Risk Management*
6.9. *Policy: Work Health and Safety*
6.10. *Policy: Information and Information Technology*
6.11. *IT Disaster Recovery Plan*
6.12. *Business Continuity Plan*

7. DEFINITIONS

7.1. **For the purpose of this Policy, the following definitions apply*:***

Critical Incident refers to a traumatic event, or the threat of such (within or outside Australia), which causes serious damage to University property and/or extreme stress, fear or injury to a staff,

student or visitor participating in any officially sanctioned University activity. It can include (but it not limited to): natural disasters; large scale fires, bushfires or explosions; bomb threats; death, serious injury, or attempted suicide; robbery; missing persons; terrorist acts; riots; toxic/chemical release or large scale damage to the environment; serious illness, pandemics and epidemics; sexual assault, kidnapping or attempted kidnapping; and major cyber security and IT security incidents. It includes a matter deemed by the Incident Controller to be dealt with as a Critical Incident under this Policy.

Note: For Critical Incidents involving International Students please reference the *Procedure Critical Incident Management* for additional requirements and compliance.

Incident Controller is the nominated officer with responsibility to control a Critical Incident at the location.

Critical Incident Management Team comprises appropriate University Staff to assume responsibility for managing and directing the Critical Incident.

Staff means all Academic and Professional staff members of the University.

Student has the same meaning as in the *General Regulations*.

8. VERSION CONTROL

Version	Date of approval	Approved by	Amendment
1	29 June 2012	Vice Chancellor	Effective date – new Policy.
2	4 August 2013	Vice Chancellor	Updated Designated Officer and Contact Details list.
3	28 October 2014	Vice Chancellor	Updated Designated Officer and Contact Details list.
4	11 May 2018	Vice Chancellor	Procedural information extracted into new Procedure document.
5	27 June 2019	Senior Operations Officer	Updated to new Policy template.
6	14 December 2022	Vice Chancellor	Major amendments – updated to align with current organisational structure and university processes, including IT recovery.
7	19 April 2023	Deputy Vice Chancellor, Finance & Chief Operating Officer	Minor amendments to include the definition of a critical incident and record keeping requirements in the National Code 2018.