Critical Incident Policy
Version 1.0

1. Purpose

Nexus Institute of Higher Education is committed to the safety, security and well-being of its students, staff and the broader community. This Policy is designed to provide clear procedures for the identification, response and recovery from critical incidents to minimise harm and maintain the continuity of education and services.

The approach to emergency preparedness and response is consistent with Australian Standard 3745-2010.

This policy should be read in conjunction with

- Business Continuity Plan
- Risk Management Policy
- Risk Register
- Health and Safety Policy
- Work Health and Safety Policy
- Sexual Assault and Sexual Harassment Prevention Policy
- Bullying, Discrimination and Harassment Prevention Policy

2. Scope

The policy applies to all students, staff and others involved in the activities of Nexus Institute.

3. Definitions

Critical incident. A critical incident is any event that poses a serious risk to the life, health or safety of an individual involved in the activities of Nexus Institute. This includes incidents where students, staff and others feel unsafe and under stress. Critical incidents include:

- Fatalities or serious injuries
- Natural disasters (for example, bushfires, floods, earthquakes).
- Man-made incidents (for example, murder, suicide, attempted suicide, assault, terrorist attacks, chemical spills, power outages, serious crime).
- Health emergencies (for example, pandemics, outbreaks, infectious diseases, a mental health emergency, a missing person).
- Safety threats (for example, violence, bomb threats, fire).
- Cybersecurity incidents (for example, data breaches, hacking).

4. Policy statement

The policy aims to ensure the safety and well-being of all members of the Institute during critical incidents. Nexus Institute fosters safety and security by assessing and controlling risks to its operations under the Risk Management Policy. Nexus Institute provides information and training to students and staff on how to seek assistance and how to report incidents.

The policy outlines a coordinated, efficient and effective response to critical incidents. Nexus Institute will provide appropriate support to students, staff and others affected by a critical incident.

The aim is to facilitate recovery and minimise disruption to academic and administrative activities. Nexus Institute will provide resources to support the resumption of normal activities as soon as possible.

The Executive Management Team, led by the CEO, will be trained in crisis management and monitor the Institute's activities for emerging threats.

Upon notification or identification of a critical incident, the CEO will form an Incident Response Team to:

- assess the situation and its impact
- develop and implement an incident-specific response plan
- communicate with staff, students, and relevant external parties as required
- issue a media release if appropriate
- ensure the safety and well-being of individuals
- document all actions taken.

After the immediate response phase, the Incident Response Team will focus on recovery and continuity efforts, which include:

- assessing damage and needs
- developing recovery plans
- resuming academic and administrative activities
- providing support and counselling services as needed
- reviewing the response to the critical incident and the response plan and identifying improvements for future incidents.

5. Procedures

Reporting. A list of emergency and security contacts will be maintained on the website.

Fatalities and serious injuries.

- The first priority is to ensure the safety and well-being of individuals present at the scene, contact emergency services (for example, ambulance, police) and inform campus security. Preserve the scene and limit access to the area if it is relevant to a police investigation or any other inquiries.
- Notify SafeWorkNSW if required. A notifiable incident is: the death of a person. a serious injury or illness, or a dangerous incident that exposes someone to a serious risk, even if no one is injured.
- A staff member will be assigned to inform the next of kin as soon as possible and offer assistance to the family.
- Counselling, support and information on resources will be provided to affected students and staff, including special consideration.
- If an international student is involved, notify the state office of DHA, update PRISMS, inform the relevant Consulate and advise the student accommodation provider.
- Document all details and seek guidance on any further necessary procedures.

- Maintain regular communication with the family to provide updates and offer any additional assistance or support they may require; coordinate with the family to determine their preferences for a memorial service, if applicable.

Natural disasters

- Identify safe evacuation routes and shelter areas and monitor emergency alerts.
- Inform staff and students about the incident, evacuation procedures and safety measures.

Man-made incidents

- In cases of threats, collaborate with local law enforcement agencies and initiate lockdown procedures if appropriate.
- Ensure safe evacuation routes and shelter areas.
- Keep staff and students informed but be cautious about sharing sensitive information.

Health emergencies

- Communicable diseases must be reported to the relevant health authority
- Develop and communicate guidelines for quarantine and isolation.
- Implement health monitoring and testing measures.
- Plan for continuity of academic and administrative activities through online platforms.

Safety threats

- Decide whether to evacuate or shelter and provide clear and concise communication for staff and students.
- Contact emergency services and follow instructions.
- Provide counselling and support for those affected by the threat.

Cybersecurity Incidents

- Activate a cybersecurity response team to contain and mitigate the breach and reduce any potential harm to individuals.
- Isolate affected systems, change passwords and secure sensitive data.
- Inform affected parties while maintaining security.
- If a data breach is likely to result in serious harm to any individuals, a decision must be made to notify the Australian Information Commissioner. Affected individuals must be informed about the contents of the notification.
- Conduct a post-incident analysis to identify vulnerabilities and prevent future breaches.

Contact information

- Emergencies 000
- Police Assistance Line (non-emergency) 13 14 44
- SafeWork NSW 13 10 50
- Department of Home Affairs 13 18 81

- Office of the Australian Information Commissioner https://forms.business.gov.au/smartforms/servlet/SmartForm.html?formCode=OAIC-NDB&tmFormVersion

6. Roles and responsibilities

The CEO is responsible for the implementation of this policy and forming an appropriate incident response team of staff with specific roles and responsibilities.

The Executive Management Team, led by the CEO, is responsible for monitoring activities and anticipating threats.

The Registrar will maintain a register of critical incidents and provide regular reports to the CEO and the Board of Directors on critical incidents and their management.

The Registrar will maintain up-to-date contact information for safety and security and ensure that regular training and awareness programs are conducted so that all members of the Institute are prepared to respond to critical incidents effectively.

Staff and students should not place themselves or others at risk of injury. All members of the Institute are responsible for promptly reporting incidents that may have an impact on safety, security or normal operations, and following emergency procedures.

7. Related information

- Higher Education Standards Framework (Threshold Standards) 2021
- Education Services for Overseas Students 2000
- National Code of Practice for Providers of Education and Training to Overseas Students 2018, Standard 6.

8. Document control

Category	Operational
HESF Standard	6.1.4, 6.2.1e, 6.2.1i, 6.2.1j
Policy name	Critical Incident Policy
Policy owner	CEO
Policy approver	Board of DIrectors
Date of approval	16 November 2023
Date of next review	1 November 2026
Change log	Version 0. Original version created on 22 October 2023.
	Version 1. Feedback from Board of Directors incorporated on 19 Nov 23.