Incident Management Policy

Emergency Assistance

If someone is in immediate danger or requires urgent medical attention, use the Emergency Assistance contacts below:

For immediate help on the Wallumattagal Campus (North Ryde) - (02) 9850 9999
For immediate help at other locations - 000
For after-hours support and assistance for students - 1800 CARE MQ (1800 2273 67)
For students overseas on exchange or placement - International SOS +61 2 9372 2468

Also refer to the Campus Security Emergencies webpage.

Section 1 - Purpose

(1) This Policy specifies the University's approach to and processes for managing incidents, including Critical Incidents.

(2) The purpose of this Policy is to:

a. provide a framework for the appropriate management of risks associated with incidents that is integrated into the University's Risk Management Framework and aligns with the requirements of the Higher Education Standards Framework (Threshold Standards) 2021 and the National Code of Practice for Providers of Education and Training to Overseas Students 2018 (National Code);
b. support the implementation of systematic and effective approaches to managing incidents, particularly those classified as Critical Incidents;
c. support the health, safety and security of the University's staff, students, visitors and broader community; and
d. provide a process for evaluating the University's responses to incidents to continuously improve response strategies and staff capabilities.

Scope

(3) This Policy applies to the management of incidents that occur at University-owned or operated sites and facilities, including but not limited to:

a. Wallumattagal Campus (North Ryde);
b. City Campus (Levels 23 and 24, Angel Place, Pitt Street, Sydney); and
c. Trafalgar Shopping Centre (1 Trafalgar Place, Marsfield).

(4) Unless the incident is under the direction and control of the operator of another location, this Policy applies to the management of an incident that results from an incident at another location where this affects:

a. the operations of the University, including the provision of services; or
b. staff or students involved in University activities (e.g. student work placements, field work, exchange or study abroad, homestay accommodation for students for whom the University has assumed welfare responsibilities

under the National Code).

(5) This Policy provides the framework for the management of risks associated with incidents. The management of specific types of incidents may be subject to their own policies, procedures and plans listed in the table to follow, which should be referred to in conjunction with this Policy. Any of these types of incidents may be classified as a Critical Incident under this Policy.

	Incident type	Policies, procedures, plans
a.	Health and safety	Health and Safety Risk Management Policy Health and Safety Risk Management Procedure Standard procedures established within University faculties and portfolios to manage specialised health and safety incidents (including laboratory, chemical, biological, nanotechnology, gas, electrical, laser, ionising radiation, workshop) (see WHS Hub)
b.	Student wellbeing	Discrimination, Bullying and Harassment Prevention Policy Gender-based Violence Prevention and Response Policy Gender-based Violence Investigation Procedure Death of Student or Staff Procedure Under 18 Welfare and Accommodation Procedure
c.	Staff wellbeing	Discrimination, Bullying and Harassment Prevention Policy Gender-based Violence Prevention and Response Policy Gender-based Violence Investigation Procedure
d.	Physical security	MQ Group Emergency Management Plan Weapons on Campus Procedure
e.	Cyber security	Cyber Security Policy Information Technology Disaster Recovery Policy
f.	Approved University travel	Travel Policy Travel Procedure Insurable Risk Policy and Insurable Risk Guideline
g.	Privacy	Privacy Policy
h.	Fraud and corruption	Fraud and Corruption Control Policy Public Interest Disclosure Policy

Section 2 - Policy

(6) The University's incident management capability is designed and implemented to include the following core elements:

a. planning and preparing - developing, documenting, training and testing arrangements;
b. detecting and mitigating - identifying, assessing, controlling, treating and monitoring risks;
c. responding - making people safe, minimising damage to assets, and managing strategic issues and consequences;
d. recovering - implementing Business Continuity arrangements and repairing negative impacts; and
e. learning and adapting - reviewing and improving arrangements.

(7) The University uses a risk-based, incident classification and escalation process in alignment with the University's Risk Assessment Matrix to define the level of response required by the University to manage incidents, as follows:

a. Level 1 (minor) incident is a local event or issue that:
    i. has no more than a minor consequence rating in any risk category and little or no potential to escalate;
    ii. can be resolved satisfactorily through standard procedures and channels; and

iii. can be managed satisfactorily at the local level by on-site personnel.

b. Level 2 (serious) incident is an event or issue that:
   i. has no more than a moderate consequence rating in any risk category but potential to escalate;
   ii. may not necessarily be resolved satisfactorily by standard procedures and channels; and
   iii. needs moderate levels of resource and input to manage, which may include a Business Continuity response.
c. Level 3 (Critical) Incident is a situation with a substantial, major or catastrophic consequence rating in any risk category and will be an event or issue that:
   i. has a long-term or profound effect;
   ii. cannot be controlled through standard procedures and channels; and
   iii. needs high levels of resources and inputs to manage, which will include the Critical Incident Management Team (CIMT) and may include a Business Continuity response.

(8) The University will maintain a trained and competent Serious Incident Management Team (SIMT) for each serious incident (level 2), and a Critical Incident Management Team (CIMT) to control the University's strategic response and provide executive decisions and strategic direction relating to a Critical Incident (level 3).

(9) The CIMT comprises:

a. Vice-Chancellor (Critical Incident Management Team Leader);
b. Chief Risk Officer (Critical Incident Management Team Coordinator);
c. Director and Chief of Staff, Office of the Vice-Chancellor;
d. Vice-President, Finance and Resources;
e. Deputy Vice-Chancellor (People and Operations);
f. Deputy Vice-Chancellor (Academic);
g. Pro Vice-Chancellor (Dean of Students);
h. Chief Information and Digital Officer, Information Technology;
i. Executive Director, Property;
j. Chief People Officer; and
k. Director, Communications.

(10) The CIMT may also comprise additional expert stakeholders as required depending on the nature of the incident.

(11) Depending on the nature of a serious incident a SIMT may comprise of:

a. Executive Group member (lead, based on the nature of the incident);
b. WHS Emergency Management Officer;
c. Campus Security Manager;
d. Head of Asset and Facilities Management, Property;
e. Head, Work Health and Safety;
f. Head, Student Wellbeing;
g. Senior Security Control Centre Operator;
h. Chief Information Security Officer, IT;
i. Faculty of Science and Engineering technical representative;
j. Director of Nursing, Macquarie University Health;
k. Chief Executive Officer, U@MQ Ltd; and/or
l. Deputy Director, Human Resources and Head, Human Resources Client Services.

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.

(12) The SIMT may also comprise additional expert stakeholders as required depending on the nature of the emergency, as determined in the relevant Response Plan or 'Playbook'.

(13) The University will complete periodic training and testing of the University's incident management teams and associated systems or capabilities.

Responsibilities

(14) The Vice-Chancellor is the University's Critical Incident Lead and is responsible for leading the CIMT and overseeing the implementation of the MQ Group Critical Incident Management Plan.

(15) The Chief Risk Officer is the University's CIMT Coordinator and is responsible for:

a. facilitating the implementation of the Critical Incident Management Plan;
b. coordinating the CIMT; and
c. managing serious and Critical Incident training, testing and compliance.

(16) Responsibilities for managing specific incidents are to be carried out in accordance with existing delegations as specified in the University or relevant controlled entity's Delegations of Authority Register, and the policies specified in clause 5.

Section 3 - Procedures

Reporting and classifying incidents

(17) Incidents are reported through a variety of mechanisms depending on the nature of the incident. Mechanisms include:

a. Risk and safety reporting (in Protecht software) for health and safety incidents;
b. Student CARE MQ referral for a range of student-related incidents;
c. Macquarie University Health email to the Patient Safety and Quality Team;
d. contacting Security Services or other relevant University office or unit; or
e. complaints lodged in accordance with the Complaints Resolution Procedure for Students and Members of the Public or Complaint Management Procedure for Staff.

(18) A preliminary classification of all reported incidents as Level 1, 2 or 3 is made by the incident report receiver according to the risk-based classifications specified in clause 7.

(19) The incident report receiver will urgently direct incidents with a preliminary Level 2 or 3 classification to the relevant incident response team.

(20) The incident response team will:

a. review incidents and determine their classification;
b. respond to, manage and stabilise incidents in accordance with the relevant incident plan, policy or procedure (as specified in clause 5); and
c. direct incidents with a preliminary Level 3 classification to the Critical Incident Management Team (CIMT) Coordinator and Leader for formal incident classification and further action.

(21) The classification of an incident may be escalated or de-escalated by the relevant incident management team.

(22) The CIMT Coordinator and Leader will evaluate the reported incident and, where the incident is determined to be a Critical Incident (Level 3), will activate the CIMT.

(23) Where appropriate the CIMT Leader may consult:

a. relevant State or Commonwealth government agencies including NSW Police, NSW Fire and Rescue, NSW Ambulance, NSW Health, Australian Cyber Security Centre, or the relevant Commonwealth Department (e.g. Department of Foreign Affairs and Trade);
b. travel warnings issued through International SOS, SmartTraveller, or the University's approved travel management company;
c. relevant embassies and consulates; and
d. Faculties and Portfolios of the University to determine the impact of the incident, emergency or disaster to the University community and University activities.

Responding to Critical Incidents

(24) The CIMT will:

a. review the situation, set priorities, allocate tasks and responsibilities, and coordinate the University's response to the Critical Incident;
b. manage media and publicity relating to the Critical Incident, and arrangements for notifying staff, students, and other affected individuals as appropriate;
c. ensure that the incident response team has adequate support and resources to respond to and stabilise the incident;
d. seek advice from the General Counsel about any statutory obligations or external reporting obligations arising from a Critical Incident;
e. report any incident involving suspected fraud or corruption to the Vice-President, Finance and Resources in accordance with the Fraud and Corruption Control Policy; and
f. ensure that stakeholders and regulatory bodies, including but not limited to, the Tertiary Education Quality and Standards Agency (TEQSA), SafeWork NSW and the University's insurers are notified in a timely manner where required and provided with appropriate information.

(25) The release of any personal information to external parties must comply with the University's Privacy Policy.

Recovering from a Critical Incident

(26) After managing the initial response to a Critical Incident, the CIMT will review and refine, as necessary, any plans to manage the incident and put in place a recovery strategy.

(27) When an incident disrupts a critical activity or process, the University's Business Continuity processes will be implemented.

(28) Depending on the circumstances, the CIMT may be disestablished by the CIMT Leader and the matter referred to the relevant manager to enable effective continuation of services and planning for restoration to full recovery and return to business as usual.

Records of Critical Incidents

(29) The CIMT Coordinator will ensure that all actions, decisions, and accountabilities relating to a Critical Incident are managed in accordance with the Records and Information Management Policy.

(30) The CIMT Coordinator or their nominee will maintain up-to-date confidential incident records.

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.

Learning and adapting from a Critical Incident

(31) The CIMT will consider the need to establish an Incident Investigation Team in a timely manner to investigate the incident, identify its cause and contributing factors, and develop recommendations to prevent a recurrence. The composition and size of the team will depend on the nature and complexity of the Critical Incident.

(32) As soon as practicable after a Critical Incident, the CIMT will review and evaluate the effectiveness of the treatment and management of the Critical Incident.

(33) The CIMT will also review the University's Critical Incident processes at least annually and propose revisions as appropriate for implementation through the relevant channels.

(34) Responses to Critical Incidents will be reported to the University Council by the Vice-Chancellor.

Section 4 - Guidelines

(35) Nil.

Section 5 - Definitions

(36) The following definitions apply for the purpose of this Policy:

a. Business Continuity means capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
b. Critical Incident has the meaning given to it in clause 7(c).

Status and Details

Status	Current
Effective Date	2nd July 2024
Review Date	2nd July 2027
Approval Authority	Vice-Chancellor
Approval Date	2nd July 2024
Expiry Date	Not Applicable
Responsible Executive	Robin Payne Vice-President, Finance and Resources
Responsible Officer	Kylie McKiernan Chief Risk Officer
Enquiries Contact	Kylie McKiernan Chief Risk Officer

This document may be varied, withdrawn, or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Policy Central (https://policies.mq.edu.au) for the latest version.