Critical Incident Management Policy

Emergency Assistance

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

For immediate help on the North Ryde Campus - (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

(2) Also refer to the Campus Security Emergencies webpage.

Section 1 - Purpose

(3) This Policy specifies the University's approach to and processes for managing critical incidents.

(4) The purpose of this Policy is to:

a. provide a framework for the appropriate management of risks associated with critical 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 ESOS National Code;
b. support the implementation of systematic and effective approaches to managing incidents classified as critical incidents that seriously affect, or may seriously affect, the University's staff, students and visitors, property, operations, activities or reputation;
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 critical incidents in order to continuously improve response strategies and staff capabilities.

(5) This Policy forms part of and supports the implementation of the MQ Group Emergency Management framework.

Scope

(6) Subject to the facility and location exclusions specified in clause 8, this Policy applies to the management of critical incidents that occur at:

a. University-owned or operated sites and facilities at:
    i. North Ryde Campus;
    ii. Waterloo Road Precinct (44 and 50 Waterloo Road, North Ryde);
    iii. City Campus (Levels 23 and 24, Angel Place, Pitt Street, Sydney); and
    iv. Trafalgar Shopping Centre (1 Trafalgar Place, Marsfield, NSW, 2122.).

(7) Unless the critical incident is under the direction and control of the operator of another location, this Policy applies to the management of a critical 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 ESOS National Code).

(8) Critical incidents at the following facilities owned by the University are directed and controlled in accordance with the plans and procedures of the lessees or operators of those facilities and are not included in the scope of this Policy:

a. Cochlear, 1 University Avenue, Macquarie Park;
b. Panasonic, 1 Innovation Road, Macquarie Park;
c. Siemens, 160 Innovation Road, Macquarie Park;
d. 299 Lane Cove Road, Macquarie Park;
e. MQ Health Hospital and Clinics, 3 Technology Place, Macquarie University and 2 Technology Place, Macquarie University respectively; and
f. non-University student accommodation such as Dunmore Lang College, Morling College, Robert Menzies College, and Campus Living Village.

(9) This Policy provides the framework for the management of risks associated with critical incidents. The management of specific types of incidents may be subject to their own policies, procedures and plans listed in the table below, 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 Student Sexual Misconduct Prevention and Response Policy Student Sexual Misconduct Prevention and Response Procedure Death of Student or Staff Procedure Under 18 Welfare and Accommodation Procedure
c.	Staff wellbeing	Discrimination, Bullying and Harassment Prevention Policy Staff Sexual Harassment Prevention and Response Policy Staff Sexual Harassment Prevention and Response 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 Reporting Wrongdoing - Public Interest Disclosures Procedure

Section 2 - Policy

(10) The University's critical 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.

(11) The University has established and maintains a MQ Group Emergency Planning Committee (GEPC), chaired by the Vice-President, Finance and Resources. The GEPC is responsible for overseeing and maintaining the MQ Group Emergency Management Framework and its constituent plans, emergency management planning and preparation, training, review and compliance.

(12) The University uses a risk-based, critical 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 impact 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, which may include an Emergency Response Team if the incident is an emergency.
b. Level 2 (moderate) incident is an event or issue that:
    i. has no more than a moderate impact 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 and, if the incident is an emergency, an Emergency Response Team.
c. Level 3 (critical) incident is a situation with a substantial, major or catastrophic impact 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 and may include a Business Continuity response and, if the incident is an emergency, an Emergency Response Team.

(13) The University will maintain a trained and competent Critical Incident Management Team (CIMT) to control the University's strategic response and provide executive decisions and strategic direction relating to a critical incident. An incident response team, with appropriate expertise and training, will also be activated for each critical incident (e.g. Emergency Response Team (ERT) in the case of an emergency).

(14) 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. Vice-President, Professional Services;
f. Deputy Vice-Chancellor (Academic);
g. Dean of Students;
h. Chief Information and Digital Officer, Information Technology;
i. Executive Director, Property Services;
j. Chief People Officer; and
k. Director, Communications.

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

(16) The ERT comprises:

a. WHS Emergency Management Officer;
b. Campus Security Manager;
c. Head of Asset and Facilities Management, Property;
d. Manager, Workplace Health and Safety;
e. Head or Manager, Student Wellbeing; and
f. Senior Security Control Centre Operator.

(17) The ERT may also comprise additional expert stakeholders as required depending on the nature of the emergency, including:

a. Chief Information Security Officer, IT;
b. Faculty of Science and Engineering technical representative;
c. Executive Director of Nursing, MQ Health;
d. U@MQ CEO; and/or
e. Deputy Director, Human Resources.

(18) The University will complete annual training and testing of the University's CIMT and associated systems or capabilities.

Responsibilities

(19) 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.

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

a. facilitating the implementation of the Critical Incident Management Plan and the Emergency Management Plan;
b. coordinating the CIMT and GEPC; and
c. managing emergency and critical incident training, testing and compliance.

(21) Responsibilities for managing specific incidents are specified in the University or relevant controlled entity’s Delegations of Authority Register, the MQ Group Emergency Management framework and its constituent plans, and the policies specified in clause 9.

Section 3 - Procedures

(22) Any incident at the University, or affecting its operations, staff, students or other members of the University community, has the potential to start as or escalate into a Level 3 (critical) incident. Incident types include, but are not limited to:

a. events such as fire, explosion, chemical spill, gas leak, power outage, violent attack, active shooter or terror attack, fatality or injury, epidemic, natural disaster;
b. issues or events (internal or external) such as public health concerns, cyber-attack, fraud or mismanagement, or adverse behaviour by individuals; and
c. activities that may attract adverse attention from government, regulators, interest groups, the public or media.

Reporting and classifying incidents

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

a. ROAR - Risk Online Active Reporting report for health and safety incidents;
b. Student CARE MQ referral for a range of student-related incidents;
c. MQ Health email the Patient Safety and Quality Team;
d. contacting Security Services or other relevant University office or unit; or
e. lodging a complaint in accordance with the Complaints Resolution Procedure for Students and Members of the Public or Complaint Management Procedure for Staff.

(24) 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 12.

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

(26) The incident response team will:

a. review incidents and confirm their preliminary classification;
b. respond to, manage and stabilise incidents in accordance with the relevant incident plan, policy or procedure (as specified in clause 9); 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.

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

(28) Where appropriate the CIMT Leader may consult:

a. advice issued by the 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

(29) 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, parents, 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.

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

Recovering from a critical incident

(31) 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.

(32) When an incident disrupts a critical activity or process, the University's business continuity processes will be implemented.

(33) 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

(34) The CIMT Coordinator will ensure that all actions, decisions, and accountabilities relating to a critical incident are managed in accordance with the University’s Records and Information Management Policy on behalf of the CIMT.

(35) The CIMT Coordinator or their nominee will maintain up-to-date confidential incident records that will be available to members of the CIMT and other persons authorised by the CIMT Coordinator or CIMT Leader on a need-to-know basis.

Learning and adapting from a critical incident

(36) 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.

(37) The Incident Investigation Team will develop a report, in consultation with the CIMT, that includes:

a. relevant facts and evidence; and

b. recommended improvements to plans, processes, and/or training.

(38) 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. The review will be informed by the Incident Investigation Team report that includes recommendations for managing similar future critical incidents and training needs.

(39) The CIMT Coordinator will report all critical incidents to the GEPC, including recommended corrective actions and lessons learnt.

(40) The CIMT will also review the University’s critical incident processes at least annually and propose revisions as appropriate for implementation through the GEPC.

(41) Responses to critical incidents will be overseen and monitored by the University Council through the Vice-Chancellor.

Section 4 - Guidelines

(42) Nil.

Section 5 - Definitions

(43) 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 means a traumatic event, or threat of a traumatic event (within or outside Australia) or series of escalating events which causes extreme stress, fear or injury and that has the potential to significantly damage the University’s people, business operations, assets or reputation.
c. Cyber attack means an attack by digital means that targets the University's information systems or personnel with the intent of damaging, disrupting or controlling computer systems, or gaining unauthorised access to information.
d. Emergency means an unplanned or impending situation generated internally or externally that may: cause harm to people; result in significant damage or loss to the property of the University, including intellectual property; and/or result in major disruption to normal operations.
e. MQ Group means the University, and its controlled entities.
f. University activities means all activities both on and off-shore undertaken by staff, students or third parties within the management and control of the University.

Status and Details

Status	Current
Effective Date	21st June 2022
Review Date	21st June 2025
Approval Authority	Vice-Chancellor
Approval Date	20th June 2022
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