Crisis Management Procedure

Section 1 - Purpose

(1) This procedure outlines the University's crisis management model and arrangements for responding to incidents in accordance with the Resilience Policy.

(2) The procedure describes:

a. the details and principles of the crisis management model
b. the method for incident classification and activation, and when and how to establish crisis management arrangements
c. the roles and responsibilities of the senior executive team, crisis management teams and operational response teams, and how these teams operate and interact, and
d. when and how to transition incident management arrangements to business continuity plans, recovery and stand down the crisis management team.

Scope

(3) This procedure applies to all:

a. incidents that have been assessed as a Level 1-3 incident (see Part B)
b. University-related activities, and
c. senior executive leaders and other University staff who are required to respond to incidents.

Section 2 - Policy

(4) Refer to the Resilience Policy.

Section 3 - Procedures

(5) This procedure is subordinate to the Resilience Policy, as shown in the following hierarchy:

a. Resilience Policy
b. Crisis Management Procedure
c. Crisis Management Plan
d. Staff and Student Critical Incident Plans
e. Incident Playbooks

(6) The Crisis Management Plan provides the practical information for the execution of effective crisis management, and in particular, the information required to effectively run the crisis management team and operational response teams.

This document may be varied, withdrawn or replaced at any time.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 the CSU Policy Library for the latest version.

Part A - Crisis management model

(7) The University follows a three-tiered crisis management model:

Oversight	University Council maintains oversight and governance, ensures effective plans, supports the Vice-Chancellor with strategic guidance and empowers their decision-making.	
Level 3 – Strategic response	Senior executive team (SET)	Led by the Vice-Chancellor or appointee Provides strategic direction to the University's response Approves all external public communications Provides: updates to Council; decisions to tiers 2 and 3 Receives: guidance from Council
Level 2 – Tactical response	Crisis management team (CMT)	Leader appointed by senior executive Responds to incidents affecting multiple areas May convene specialist teams for legal advice, communications, etc. Provides: updates to tier 1; decisions to tier 3 Receives: decisions from tier 1
Level 1 -Operational response	Operational response teams (ORT)	Led by business as usual (BAU) leader (for normal business units) or person appointed by the CMT (when task organised) Activated in accordance with emergency plans, business continuity plans and/or as directed by the CMT Provides: updates to tiers 1 and 2 Receives: directions from tiers 1 and 2

(8) This simple and adaptable model can be tailored to a range of simple and complex scenarios, and is defined by the following key principles:

a. Adaptive support: prioritise effective support to operational response while remaining flexible.
b. Tiered Response: a tailored, graduated crisis response system.
c. Effective communication: timely reporting, decision-making and communications management.
d. All-hazard management: a simple, versatile robust system for all incident types.
e. Resource mobilisation: swift allocation of resources in support of an effective response.

Crisis management sequence and transition

(9) Four general phases will occur following an emergency event requiring a crisis response. They may occur in sequence with overlap, as above, or simultaneously, especially in the case of multiple events.

a. Operational response - to manage emergencies where an immediate internal or external emergency services response is required. Consists of the activation of drills and procedures immediately following an event to protect people, property and information from harm and raise the alarm. Physical Emergency Response is detailed by the Emergency Management Procedure.
b. Crisis management - to provide a strategic and systematic approach to the management of crises. Involves the formulation and execution of strategies designed to manage the crisis.
c. Business continuity management – to continue or re-establish critical business processes in a timely manner, in the event of a disruption. Involves the implementation of plans in order for the University to maintain critical functions during the crisis. See Business Continuity Management Procedure.
d. Recovery – refers to the restoration of business-as-usual through the rebuilding of systems and processes and ongoing management of people to return the organisation to pre-crisis levels of performance and resilience.

(10) Following stabilisation of the situation and management of the crisis phase, the CMT will seek to:

a. transition to business continuity plans which will be managed under business as usual (BAU) arrangements, and
b. facilitate effective recovery, either through management of recovery by the CMT itself, or handover to an appointed recovery management team.

Part B - Incident classification and management

(11) All incidents, following the initial emergency response in accordance with applicable plans, reported through the University's incident reporting processes are assessed by an incident assessment team and classified according to severity. This classification determines which tier of the crisis management model is required:

Emergency/incident/threat	Incident assessment team	Lvl 1	Brief to applicable senior executive	Tier 1 response required: ORTs convened
		Lvl 2	Brief to applicable senior executive	Tier 2 tactical response: CMT and ORTs convened
		Lvl 3	Brief to senior executive team	Tier 3 strategic response: SET, CMT and ORTs convened

Incident assessment and classification

(12) The University's incident reporting procedures ensure key incidents are reported through to Executive Director, Safety, Security and Wellbeing, the Director, Security and Resilience (CSO) and/or the Director, Risk and Compliance. These can occur through multiple means. Upon notification, the informed officer will activate the incident assessment team.

(13) The incident assessment team (IAT) is a small, qualified team that assesses and classifies the incident. It consists of:

a. a senior executive leader (e.g. Vice-Chancellor or a portfolio lead)
b. Director, Risk and Compliance, or their representative
c. Executive Director, Safety, Security and Wellbeing, and/or the Director, Security and Resilience (CSO)
d. the relevant area director or head for the business area in which the incident occurred, or partnership representative where relevant (e.g. Director, Facilities Management for physical incidents).

(14) This team assesses the incident using the incident severity tool contained in the Crisis Management Plan.

(15) Once the incident is classified, the IAT briefs the relevant senior executive leader and/or SET and the appropriate tier response is activated (see table at clause 11).

(16) Notwithstanding the IAT assessment and classification, any senior executive leader may activate a CMT at any time.

Incident classification table

(17) Incidents will be classified according to the following table, supported by an incident assessment:

Incident classification	Response team	Description	Incident management structure	Examples
Level 0 – Adverse event	Business as usual (BAU)	Low risk Routine business activities Minor issues with minimal impact Low complexity Standard operating procedures apply Can be managed within BAU structure Line reporting is sufficient No significant impact on operations	Managed internally in accordance with BAU structures line reporting	Example: fire alarm evacuation with no fire.
Level 1 - Incident	Operational response teams (ORT)	Moderate risk Potential for operational disruption but manageable Some impact on normal activities Low complexity Requires some coordination among teams	Managed within internal emergency/incident structures line and IAT reporting Business continuity/incident plans enacted	Example: minor fire with no injuries, no damage causing significant operational effects, evacuation etc. effective, no media coverage
Level 2 – Critical incident	Crisis Management Team (CMT)	High risk Significant potential for disruption Requires immediate attention and intervention Moderate complexity, potentially affecting partnerships Significant, rapid coordination required across multiple sections of the University	CMT activated with ORT's subordinated and directed by the CMT CMT reporting to senior executive (portfolio leader)	Example: significant fire resulting in minor injuries and damage to a significant amount of equipment, with some media exposure
Level 3 - Crisis	Senior executive team (SET)	High risk Critical situation impacting the entire organisation Potential for severe reputational damage High complexity, potentially affecting multiple partnerships Requires the highest level of organisational response Intensive communication and coordination efforts across the organisation	CMT active and subordinated to SET SET guiding the organisational response, approving plans for execution by the CMT, and briefing University Council	Example: significant fire affecting multiple buildings, causing significant injuries, significantly disrupting University operations and gaining considerable media coverage

Part C - Crisis management tiers

Tier 1: Operational response – Operational response teams

Note: In the event of an emergency, emergency response teams may already be activated and managing the incident under the Emergency Management Procedure and emergency plans.

(18) Operational response teams (ORTs) include the emergency control organisation under the Emergency Management Procedure, as well as teams identified in business continuity plans or ad hoc teams as determined by the senior executive leader or CMT.

(19) In a Level 1 response, ORTs report through their line reporting. In Level 2 and 3 responses, they are subordinated directly to the CMT.

(20) ORTs have the following responsibilities:

a. Emergency management (emergency control organisations)
    i. Immediate response to incidents on the ground.
    ii. Execute predefined emergency protocols to address the situation promptly to preserve safety and property.
b. Student and staff critical incident management
    i. Prioritise the safety and well-being of students and staff.
    ii. Implement crisis response plans tailored to the specific incident in accordance with the Student Critical Incident Plan.
    iii. Support international students, where applicable, in accordance with Standard 6 of the National Code of Practice for Providers of Education and Training to Overseas Students.
c. Other teams
    i. Execute business continuity plans where applicable.
    ii. Collaborate with relevant teams to coordinate a cohesive response.
    iii. Utilise specialised skills and resources to address specific aspects of the incident.
d. Preserving life and minimising harm
    i. Focus on immediate actions to protect lives, property and information and minimise harm.
    ii. Provide timely and accurate information to affected individuals.

Tier 2: Tactical response – Crisis management team

(21) The crisis management team (CMT) consists of the appointed leader and a task-organised team from across the University, in accordance with the Crisis Management Plan. It is facilitated by the Director, Security and Resilience (CSO).

(22) The CMT will:

a. Provide operational support and guidance
    i. Support and guide ORTs.
    ii. Ensure alignment with overall incident response objectives.
b. Maintain communications
    i. Facilitate clear communication between front-line responders and the CMT.
    ii. Relay critical information and updates to all relevant parties.
c. Make operational decisions
    i. Authorise operational decisions within delegated authority.
    ii. Act promptly to address issues and keep the response effective.

d. Meet administration practices
    i. Adhere to proper meeting administration practices.
    ii. Prepare documentation and maintain records for accountability and analysis.
e. Refer matters beyond authority
    i. Identify issues exceeding delegated authority.
    ii. Refer such matters to the SET for higher-level consideration and decisions.

Tier 3: Strategic response – Senior executive team

(23) The senior executive team (SET) consists of members stated at the 'Senior executive team (SET) roles and management' heading below.

(24) The SET will:

a. Provide strategic leadership
    i. Oversee the strategic direction of crisis response efforts, setting clear goals and priorities for the CMT.
    ii. Communicate with University Council.
b. Manage strategic and reputational impacts
    i. Address strategic and reputational implications of the crisis, including oversight and approval of public communication.
    ii. Formulate strategies to mitigate long-term impacts on the University.
c. Ensure risk management
    i. Ensure that risk is managed in alignment with University Council direction.
    ii. Escalate critical risk issues to the University Council when necessary.
d. Approve working arrangements
    i. Have the authority to approve and provide clarity on working arrangements.
    ii. Adapt policies and procedures as needed during the crisis.
e. Meet as required
    i. Convene meetings based on advice from the CMT Leader.
    ii. Meet as directed by the Vice-Chancellor to address strategic decisions and updates.

Senior executive team (SET) roles and management

(25) The SET consists of the:

a. Leader: Vice-Chancellor (or properly authorised delegate)
b. Portfolio leaders: Chief Operating Officer, Provost and Deputy Vice-Chancellor (Academic), Deputy Vice-Chancellor and Vice-President (Research)

(26) When the SET meets it is joined by the below as required:

a. CMT leader: the nominated leader of the CMT.
b. Facilitator: primary – Director, Security and Resilience (CSO), secondary – Chief of Staff, emergency – Director, Risk and Compliance, Executive Director, Safety, Security and Wellbeing
c. Executive support: an appropriate Executive Officer or Executive Assistant
d. University Secretary
e. Media and communications: Chief of Staff, Head, Communications and Government Relations

f. Support roles as required, including other key CMT staff.

(27) A secured Microsoft Teams group is in place for the conduct of SET briefings. Should Microsoft Teams be unavailable, a suitable alternative will be set up by the CMT.

(28) Briefings will include:

a. situation brief
b. proposed crisis management plan
c. key risks
d. senior executive team plan amendment and endorsement.

(29) Further details related to the briefings, including templates and considerations, are included in the Crisis Management Plan.

Communications management

(30) External communications are managed as follows:

a. For activities from Level 2 – Level 3, an integrated approach to communication will be led by the CMT. This includes students, staff, stakeholders and media.

Level 0	Level 1	Level 2	Level 3
IAW BAU structures – no public communication with the exception of campus alerts. Contacts Manager, Digital and Social Media if contacted by media	Head, Communications and Government Relations determines point of communication handover back to BAU owner and support to finalise	Head, Communications and Government Relations	Chief of Staff directs all communication with support of Head, Communications and Government Relations to execute

(31) External public communication will only occur with the approval of the Vice-Chancellor's office, through the Chief of Staff, even in situations where the CMT is activated. This is with the exception of Level 0 incidents when communication channels including campus alerts will be issued directly by the operational response teams involved.

a. In the event that the Chief of Staff is on leave or unavailable, the University Secretary or Head, Communications and Government Relations is the successor.
b. In the event that the Head, Communications and Government Relations is on leave or unavailable, the Executive Director, Engagement and Enterprise is the successor.
c. In the event that an external regulator or agency needs to be informed of an incident, the relevant University contact will communicate with that agency following approval of messaging by the portfolio leader.

Partnerships

(32) The crisis management model described above will also be employed by the University in instances involving partners. It is understood that in these instances the University’s and the partner’s crisis management processes will be required to run in parallel.

(33) This will be coordinated by the placement of suitable liaison staff (e.g. partnership managers) onto the CMT and equivalent groups within partner organisations. In some instances, it may be appropriate, if agreed between the University and the partner, to run a combined CMT.

Review and reporting

(34) An after-incident review will be conducted following all Level 2 and Level 3 incidents. Details for the conduct are in the Crisis Management Plan.

(35) This procedure will be reviewed annually and following any significant recommendations as a result of an after-incident review.

(36) The University's crisis management model will be tested by an external party no less than once annually to Level 3 to ensure effectiveness.

(37) Level 2 and Level 3 incidents will be reported to Audit and Risk Committee in the quarterly Division of Safety, Security and Wellbeing report, along with results from tests.

Section 4 - Guidelines and other supporting documents

(38) This procedure is supported by:

a. Crisis Management Plan
b. Incident playbooks
c. Student Critical Incident Plan

Section 5 - Glossary

(39) Nil.

Section 6 - Document context

Compliance drivers	N/A
Review requirements	Annual review
Document class	Governance

Status and Details

Status	Current
Effective Date	9th April 2024
Review Date	9th April 2025
Approval Authority	University Secretary
Approval Date	9th April 2024
Expiry Date	Not Applicable
Unit Head	Stacey Jenkins Executive Director, Safety, Security and Wellbeing
Author	Frank Tamsitt Chief Security Officer
Enquiries Contact	Frank Tamsitt Director, Security and Resilience (CSO)

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 the CSU Policy Library for the latest version.