Critical Incident Management Guidelines

Section 1 - Purpose

(1) In accordance with the University's Resilience Policy and Resilience Framework, the purpose of these guidelines is to set out:

a. when and how to establish and stand up a Critical Incident Management Team,
b. how the Critical Incident Management Team is intended to operate, and
c. when and how to transition incident management arrangements to recovery and stand down the Critical Incident Management Team.

(2) These guidelines have been developed with the most complex and extensive critical incident management support requirements in mind. It is anticipated that the breadth and depth of this response can and will be adapted to suit the nature of the specific incident under consideration.

(3) These guidelines are intended to guide the response to a crisis incident not otherwise planned for by the University. The University has documented several purpose-specific plans to respond to anticipated crises, those plans are listed as associated information to these guidelines.

Scope

(4) These guidelines apply to the members of any Critical Incident Management Team established by the University.

(5) These guidelines are closely connected to the Crisis Management Guidelines. Any changes to these guidelines should be considered for inclusion and/or impact on those guidelines.

Section 2 - Glossary

(6) Refer to the Resilience Policy.

Section 3 - Policy

(7) Refer to the Resilience Policy.

Section 4 - Procedures

(8) Nil.

Section 5 - Guidelines

Crisis management structures

(9) The Resilience Policy identifies critical incident management processes to be overseen by a Critical Incident Management Team (CIMT).

(10) The CIMT is primarily an operational management structure intended to support the Crisis Management Team through the delegated responsibility to oversee and advise front line incident responders across the organisation.

(11) A CIMT is established if and when required by the Crisis Management Team. Where a CIMT is not established by the Crisis Management Team, the Crisis Management Team retains the role and responsibility of the CIMT.

(12) The CIMT may only act within the delegated authority of the members of the team and must at all times follow standing policy and procedure. Any variations to adopted practice must be referred to the Crisis Management Team for consideration and decision.

(13) The CIMT do not have responsibility for a strategic response to an incident impacting the University, and as such do not have authority to make public statements to internal or external stakeholders in relation to incident management or response. All such communications remain the responsibility of the Crisis Management Team.

(14) The CIMT may, and are expected to, provide strategic advice to the Crisis Management Team for their consideration and action.

Critical incident notification

(15) It is not possible to anticipate every combination of circumstances that may result in the requirement to establish incident management arrangements for the University. It has also been demonstrated that despite the most rigorous of written procedures relating to incident notification, there are inevitably numerous ways in which senior staff may become aware of a significant incident. The University's various resilience plans may set out notification processes for incident responders to follow in order to alert the Crisis Management Team of an incident but it is relevant to note that a senior staff member may become aware of an incident through a variety of means.

(16) All staff should be aware of incident notification protocols and the mechanisms for reporting.

(17) Senior staff are expected to contact their portfolio leader on becoming aware of a serious incident. It is expected that senior staff, particularly those who report directly to a portfolio leader will have direct contact details to be able to make this notification out of hours.

Standing up the Critical Incident Management Team (CIMT)

(18) Crises are managed and overseen by the Crisis Management Team according to the Crisis Management Guidelines. Depending on the extent and complexity of the incident the Crisis Management Team Leader may stand up a Critical Incident Management Team (CIMT) to provide operational support to the front line incident responders.

Critical Incident Management Team members

(19) The CIMT leader is the portfolio leader from the area primarily impacted by the incident. The portfolio leader may delegate this role to a suitably experienced senior staff member.

(20) The membership of the CIMT is intended to be flexible and responsive to the nature of the incident. It is recommended that the following functional business areas be considered for representation on the CIMT:

a. Academic portfolio administration
b. Academic portfolio leadership

c. External engagement
d. Facilities Management
e. Finance
f. Information Technology
g. Office of Global Engagement
h. Office of the Vice-Chancellor
i. People and Culture
j. Public Relations and Communications
k. Research portfolio leadership
l. Research Portfolio administration
m. Risk and Compliance
n. Security
o. Security, Safety and Wellbeing
p. Student Administration
q. Student service providers (academic and non-academic)

(21) The CIMT leader is to ensure adequate provision is to be made for the administrative support of the team. This support includes the preparation of agendas and the recording and retaining of minutes for all meetings, with special consideration of all decisions made and actions to be progressed.

(22) The CIMT leader is to use whatever resources are available to them to advise personnel that they have been appointed to a CIMT and provide information as to initial meeting arrangements.

Role of the Critical Incident Management Team

(23) The role of the CIMT is to:

a. provide operational support and guidance to the front line incident responders with the objectives of:
    i. preserving life and minimising harm to all persons,
    ii. ensuring ongoing compliance with University obligations,
    iii. minimising loss and damage to University assets and infrastructure,
    iv. minimising the extent and duration of any disruption, and
    v. supporting an orderly transition to the recovery from an incident including the re-establishment of business as usual operation,
b. maintain communications between the front line responders and the Crisis Management Team,
c. make any required operational decisions and authorise actions within the delegated authority of each CIMT member,
d. observe appropriate meeting administration practices including the preparation of meeting documentation and the retention of all relevant records, and
e. refer all matters beyond the delegated authority of the members to the Crisis Management Team for consideration and decision.

Meeting arrangements

(24) Once the Crisis Management Team leader has determined to stand up a CIMT the team is to assemble:

a. given the distributed regional footprint of the University, the most likely means of assembling the team is through an online digital platform:

i. If conventional access to Zoom is not available, go to https://charlessturt.zoom.us/ from any device and follow the options to create (or join) a Zoom meeting. The meeting host can invite participants or obtain the meeting code to provide to other CIMT members.
ii. For OneDrive access to Incident Preparedness resource materials go to https://office.com from any device and log in with your Charles Sturt credentials.

b. these arrangements rely on CIMT members having access to an internet enabled device with (battery) power:
i. A mobile phone with hotspot capability can be used to access the internet over the mobile network.
ii. To access the Incident Preparedness OneDrive, one of the two Sydney based data centres must be operational to go through the University user identity authentication systems.

Primary phase of incident support

(25) The CIMT leader is to identify the incident controller, this is the person with primary responsibility for executing the incident response at the scene.

> Note that in the event of an emergency incident where the facility emergency plan is activated, the Chief Warden is the incident controller until the all clear is declared. The Chief Warden has absolute authority to issue instructions to direct and evacuate all persons from buildings and/or other areas of the University.

(26) The CIMT administrative support officer is to follow the actions and activities of the CIMT leader and is to ensure:

a. a detailed sequence of events is recorded for the incident, including date and time stamps. Matters to be incorporated in the sequence of events include:
i. communications between key stakeholders,
ii. the occurrence of milestone events that establish the course of the incident,
iii. details of review meetings, including attendees and nature of discussions, and
iv. the decisions relating to determining a course of action, including the rationale for decision making, and
b. that action items are identified, assigned to a person, tracked through to completion and a status report is available for the CIMT leader's reference.

(27) A comprehensive and accurate sequence of events is critical to the effectiveness of post incident review and debrief and may be required for external agency investigation, especially if the incident involves criminal activity or death or serious injury of a person.

(28) The CIMT leader is to establish communication arrangements with a primary representative of the front line incident responders. This representative should be selected on the basis of:

a. availability to provide updates through the course of the incident without impacting on capacity to carry out incident response, and
b. access to accurate and timely information regarding the status of the incident.

(29) In the initial incident response phase the CIMT leader is to focus on:

a. relieving the incident responders of activities which detract from their capacity to carry out incident response,
b. providing the Crisis Management Team with regular updates,
c. maintaining accurate information regarding the extent of incident impact or loss arising from the incident,
d. containment to minimise impact and/or to prevent escalation horizontally or vertically,
e. ensuring the front line responders have the required level of resources to mount an appropriate incident

response, and

f. the welfare of persons impacted by and responding to the incident.

(30) A preliminary debrief should be conducted at the conclusion of the initial phase of the incident response.

(31) The CIMT leader is to ensure accurate records are made and retained to document the University's response to the incident and, in the first instance, a detailed and timed sequence of events should be compiled by the administrative support function of the CIMT.

Information coordination

(32) Depending on the complexity of the incident response and the likely duration of the requirement for CIMT incident support, the CIMT leader may establish information management practices guided by the following subject areas:

a. Current operations - showing all tasks currently being carried out and actions required for follow up.
b. Contacts - used to record important contact information in regular use.
c. Resource allocation - recording resources location, resources committed and resources available.
d. CIMT roster (incl breaks) for protracted assembly of the CIMT.

Secondary phase of incident support

(33) Once the initial phase of the incident concludes and the response environment becomes less urgent, the CIMT may continue providing operational support to personnel performing response activities through more conventional business as usual processes.

(34) The CIMT leader is to determine the ongoing activities of the team, including a revision of the required membership. It is intended that the CIMT be a flexible body established on a bespoke basis to respond to the incident at hand.

Stand down of the Critical Incident Management Team

(35) CIMT operations are to continue until the Crisis Management Team leader formally stands down the CIMT.

(36) Stand down of the CIMT should occur at whatever point in time the recovery phase can be managed under business as usual operational arrangements. In some cases, this may be at the commencement of the recovery phase, at an intermediate point in the recovery phase, or at the end of the recovery phase.

Transition to recovery phase

(37) The Resilience Policy outlines the strategies, processes, oversight and implementation that is required to recover from an incident. The recovery phase is characterised by the return to business as usual operations and the restoration of services.

(38) The recovery phase can be supported by a recovery team with a clear articulation of membership, responsibilities, reporting requirements and expected timeframes for completion. The exact requirements will be determined by the Crisis Management Team on an incident by incident basis.

Incident debrief

(39) A formal debrief is required at the conclusion of the CIMT operations to identify and document improvements to any aspect of the Resilience Framework and the incident oversight and response structures.

Associated information and record requirements

(40) Records relating to the response made by the University to any crises incident in accordance with the Resilience Framework are to be retained in a unique folder in UniRecords at

STRATEGIC MANAGEMENT AND EXTERNAL RELATIONS – Implementation – Resilience

(41) The Risk and Compliance Unit hold the electronic copies of the plans and protocols identified as the associated information to these guidelines. It is the responsibility of the various plan owners to ensure the Risk and Compliance Unit are provided with the most recent version of these documents for attachment to these guidelines.

(42) Copies of associated information are to be retained in the relevant folder in UniRecords at

STRATEGIC MANAGEMENT AND EXTERNAL RELATIONS – Planning – Resilience

(43) Records relating to critical incident management must be retained for a minimum of seven years unless a longer duration is specified under the NSW general disposal authorities.

Status and Details

Status	Current
Effective Date	22nd June 2022
Review Date	22nd June 2025
Approval Authority	University Secretary
Approval Date	21st June 2022
Expiry Date	Not Applicable
Unit Head	Anthony Heywood University Secretary
Author	Kim Broadley Associate Director, Compliance 34988
Enquiries Contact	Risk and Compliance Unit