THE UNIVERSITY OF NOTRE DAME AUSTRALIA

# Procedure:

## Critical Incident Management

Effective: 19 April 2023

Audience: Staff

Policy Category: Governance
Policy Sub-category: Health, Safety and Wellbeing

| | |
|---|---|
| Key words: | Critical incident |
| Procedure Owner: | Deputy Vice Chancellor, Finance & Chief Operating Officer |
| Responsible Officer: | Chief Property and Facilities Officer |
| Review Date: | December 2025 |

# Contents

## 1 PURPOSE

**1.1** This Procedure outlines the processes to be followed in response to or during a Critical Incident and in the period immediately following an incident and for the management of longer-term consequences of such an incident, and is designed to ensure that the University:

1.1.1 Meets its duty of care obligations in providing the highest possible standard of health and safety.

1.1.2 Can respond swiftly and effectively in the event of a Critical Incident, disaster or crisis.

**1.2** In the event of a Critical Incident, staff and students should follow this Procedure and also exercise common sense ensuring that the safety of all concerned is given priority.

## 2 RELATED POLICIES AND REGULATIONS

**2.1** This Procedure should be read in conjunction with related policies and procedures as prescribed in section 6 of the Critical Incident Management Policy.

## 3 CRITICAL INCIDENTS – Definitions

**3.1** As defined in the Critical Incident Management Policy, a Critical Incident refers to a traumatic event, or the threat of such (within or outside Australia) which causes serious damage to University property and/or extreme stress, fear or injury to a staff member, student or visitor participating in any officially sanctioned University activity. Incidents will be classified as a 'Critical Incident' by the Incident Controller (**IC**).

**3.2** Critical Incidents can include (but are not limited to):

- Natural disasters
- Large scale fires, bushfires or explosions;
- Bomb threats;
- Death, serious injury, or attempted suicide;
- Robbery;
- Missing persons;
- Terrorist acts;
- Riots;
- Toxic/chemical release or large scale damage to the environment;
- Serious illness, pandemics and epidemics;
- Domestic violence, sexual assault, kidnapping or attempted kidnapping;
- Severe verbal or psychological aggression; and
- Major cyber security and IT security incidents e.g. hacking, ransomware, etc.

**3.3** In relation to overseas student's, a traumatic event, or the threat of such (within or outside Australia), that could affect the overseas student's ability to undertake or complete a program such as but not limited to incidents that may cause physical or psychological harm.

**3.3** Critical Incidents may be categorised to three levels as per the table below. The IC should consider the criticality level when deciding if an incident is a Critical Incident.

| Criticality Level | Detailed Description |
|---|---|
| **Gold Level** | Major incidents of a scale that the University may be unable to deliver a substantial element of its core operations; may require the large-scale deployment of emergency services; may impact directly or indirectly most staff and/or students; and/or may pose a significant threat to University assets and/or financial results. There may be a significant threat to the reputation of the University and/or have potential serious legal ramifications. |
| **Silver Level** | Serious incidents of a scale that the University may be unable to deliver a discrete portion of core operations; may require the small-scale deployment of emergency services; may impact directly or indirectly significant numbers of staff and/or students; and/or may pose a threat to University assets and/or financial results. There may be a threat to the reputation of the University and/or have potential legal ramifications. |
| **Bronze Level** | A relatively minor or local incident causing no serious physical threat to staff, students, operations, assets, or reputation. Whilst there may be a limited disruption in services, there are no legal ramifications and minimal threat to the University's reputation. |

## 4 RESPONDING TO A POTENTIAL CRITICAL INCIDENT

***Campus-related Incidents***

**4.1** **First Response:** A staff member involved in, witnessing or becoming aware of a potential campus-related Critical Incident must immediately contact Security on the relevant campus using the following numbers. Where the potential Critical Incident involves a threat to the University as a whole, Security on each campus should be notified.

| Campus | Telephone |
|---|---|
| **Fremantle** | Ext 2123 or 0438 923 955 |
| **Broome** | Ext 3600 or 0408 962 889 |
| **Sydney** - Broadway<br>**Sydney** - Darlinghurst | 0403 458 011<br>0406 318 213 |
| **Clinical Schools** and **Liverpool office** | 0403 458 011 |

**4.2** **Escalation:** Security (or by agreement the staff member) must contact the relevant external Emergency Services and the University Logistics, Security & Facilities Officer on the following numbers. Security will attend the incident, provide a report to Emergency Services and notify the IC – refer to Section 4.10.

| Fremantle (WA) Campus – Emergency Contact Numbers | |
|---|---|
| **Police** (Life threatening emergencies) | **000** |
| **Police** (Police assistance 24/7) | **131 444**<br>**International callers:** +61 8 9351 0699<br>**Interstate callers:** (08) 9351 0699 |
| **Fire** (Emergencies) | **000** |
| **Fire** (Fremantle) | **(08) 9335 6262** |
| **Ambulance** (Life threatening emergency/injury) | **000** |
| **Logistics, Security & Facilities Officer** | **0404 084 579 / 0460 002 845** |

| Broome (WA) – Campus – Emergency Contact Numbers | |
|---|---|
| **Police** (Life threatening emergencies) | **000** |

| Broome (WA) – Campus – Emergency Contact Numbers | |
|---|---|
| **Police** (Police assistance (24/7)) | **131 444**<br>**International callers:** +61 8 9351 0699<br>**Interstate callers:** (08) 9351 0699 |
| **Fire** (Emergencies) | **000** |
| **Fire** (Broome) | **(08) 9192 1393** |
| **Ambulance** (Life threatening emergency/injury) | **000** |
| **Logistics, Security & Facilities Officer** | **0404 084 579 / 0460 002 845** |

| Sydney (NSW) Campus – Emergency Contact Numbers | |
|---|---|
| **Police** (Life threatening emergencies) | **000** |
| **Police** (Police assistance (24/7)) | **131 444**<br>**International callers:** +61 2 8303 5199<br>**Interstate callers:** (02) 8303 5199 |
| **Fire** (Emergencies) | **000** |
| **Fire** (Redfern) | **(02) 9698 1161** |
| **Ambulance** (Life threatening emergency/injury) | **000** |
| **Logistics, Security & Facilities Officer** | **0404 084 579 / 0460 002 845** |

**4.3 Logistics, Security & Facilities Officer's First Actions:**

4.3.1 Attend the location, assess the situation and determine next actions;

4.3.2 Offer immediate assistance to persons involved in the incident;

4.3.3 Ensure access for Emergency Services and obtain the names of persons involved in the incident; and

4.3.4 Document details of the incident.

4.3.5 Include opportunities for urgent debriefs and referral to appropriate supports internal or external for staff and students

***Student-related Incidents***

**4.4 First Response:** A staff member involved in, witnessing or becoming aware of a potential student-related Critical Incident must:

4.4.1 Immediately take appropriate action to protect life or protect injury to person, self or others.

4.4.2 Notify Security. Security will contact Emergency Services, the University Logistics, Security & Facilities Officer, and the IC as appropriate (in accordance with sections 4.1, 4.2 and 4.3).

4.4.3 Inform the relevant student's Faculty supervisor and/or Pro Vice Chancellor Student Experience.

**4.5** The relevant Faculty supervisor and/or Pro Vice Chancellor Student Experience should notify the Director, Student Engagement and Support and the National Counselling Coordinator to provide appropriate support and or debriefing via the Student Counselling Service.

**4.6** Where an overseas student is involved in a critical incident, the Director, Student Engagement and Support is (or delegate) also responsible for, as required:

4.1.1 Liaising with relevant embassies and consulates to ensure contact with, and support for, the family in the student's home country, and in the case of a serious accident, illness, or death, discuss allocation of roles and responsibilities.

4.1.2 Notifying the Department of Home Affairs, and any other relevant Commonwealth, State or

Territory agencies.

4.1.3 Notifying the Overseas Student Health Cover Provider.

4.1.4 In the event the student is missing or unable to be contacted, attempting to locate the student by, as required:

- notifying the police as soon as practicable
- contacting the student's parent or legal guardian to ascertain if contact has been made, and
- where the student is a Study Abroad student, contacting their Home University to ascertain if contact has been made with the emergency contact/next of kin.

4.1.5 Where there are concerns for the welfare of an overseas student under 18 years of age, confirming their accommodation and welfare arrangements, or arranging emergency accommodation and alternative welfare arrangements.

***Staff-related Incidents***

**4.7** **First Response:** A staff member involved in, witnessing or becoming aware of a potential staff-related Critical Incident must:

4.7.1 Immediately take appropriate action to protect life or protect injury to person, self or others.

4.7.2 Notify Security. Security will contact Emergency Services, the University Logistics, Security & Facilities Officer, and the IC as appropriate (in accordance with sections 4.1, 4.2 and 4.3).

4.7.3 Inform the relevant staff member's supervisor and/or Pro Vice Chancellor People & Culture.

**4.8** The relevant supervisor and/or the Pro Vice Chancellor People & Culture will ensure support for and or debriefing of the affected staff member as appropriate.

***Cyber-related Incidents***

**4.9** **First Response:** A staff member involved in, witnessing or becoming aware of a potential cyber-related Critical Incident including any suspected or actual breach of information security policy or systems must immediately report it to the Notre Dame IT Service Desk via the IT Service Portal.

**4.10** **Escalation:** The IT Service Desk will invoke the Cyber Incident Response Plan:

4.10.1 The Director, IT Business Partners & Security will be updated on the event as appropriate, should a suspected breach involve a member of staff relating to a sensitive issue. The Director, IT Business Partners & Security will inform the IC – refer section 4.10.

4.10.2 When reporting a cyber incident, it is important to collect as much information about the incident as possible to enable the Service Desk to give the incident an initial priority. Key information to be captured should include:

- Contact information of the person reporting the incident and related parties;
- Host names and IP addresses of suspected breached systems;
- Nature of incident;
- The potential impact of the incident along with which business area/s likely to be affected; and
- Description of the activity and supporting evidence.

***Incident Controller's First Responsibilities***

**4.11** **Incident Controller's First Actions:**

4.11.1 The IC is required to:

- Confirm the incident is to be dealt with as a Critical Incident under this Procedure;
- Communicate this to the Deputy Vice Chancellor, Finance & Chief Operating Officer or Vice Chancellor as soon as reasonable; and
- Convene the Critical Incident Management Team (CIMT) as required.

4.11.2 Control the situation and liaise with the relevant subject matter expert.

## 5 ACTIVATION OF THE CRITICAL INCIDENT MANAGEMENT TEAM (CIMT)

**5.1** **Activation by the Incident Controller (IC):** Depending on the scope of the incident, the IC will determine if it is a Critical Incident, communicate this to the Deputy Vice Chancellor, Finance & Chief Operating Officer or Vice Chancellor, and convene the Critical Incident Management Team (CIMT).

**5.2** **Notify and activate CIMT members:** The IC will notify and activate the CIMT (refer to Section 6 for full breakdown of CIMT roles and responsibilities and contact details). CIMT members will identify if they are responding. This will assist in identifying if any deputies are required to stand in for CIMT members.

**5.3** Depending on the incident, the IC will advise on a physical location and/or arrange a virtual option for CIMT members to meet. The following physical locations have been made available:

| Location | Contact Details |
|---|---|
| Fremantle, WA | **Primary**<br>ND48/105 (GF Meeting Room)<br>Direct Tel: 08 9433 0565 (Ext 2565)<br>(Back Up Phone = Virtual Command Centre)<br>**Backup**<br>ND50/113 (GF Reception/Lounge)<br>Direct Tel: 08 9433 0580 (Ext 2580)<br>(Back Up Phone = Virtual Command Centre) |
| Broome, WA | **Primary**<br>NDB8/112 (GF Kaillis Room)<br>Direct Tel: 08 9192 0600 (Ext 2600)<br>(Back Up Phone = Virtual Command Centre)<br>**Backup**<br>NDB11/L13 (GF Lecture Room)<br>Direct Tel: 08 9192 0638 (Ext 2638)<br>(Back Up Phone = Virtual Command Centre) |

| Location | Contact Details |
|---|---|
| NSW | **Primary**<br>NDS5/402 (Level 4, Meeting Room)<br>Direct Tel: 02 8204 0434 (Ext 4434)<br>(Back Up Phone = Virtual Command Centre)<br>**Backup**<br>NDS14/701 (Level 7, Governor's Boardroom Room)<br>Direct Tel: 02 8204 0310 (Ext 4310)<br>(Back Up Phone = Virtual Command Centre) |
| Virtual Command Centre | **Zoom Details**<br>Meeting ID: 89241223397<br>H323/SIP Password: 893925 |

## 6 CIMT – ROLES & RESPONSIBILITIES

**6.1** **CIMT Roles & Responsibilities**: The relevant roles and responsibilities of CIMT Members (and their respective deputy/secondary contacts if unavailable) are captured in the table below. Additional resources may be requested as required.

| Contact Details (as of August 2022) | | |
|---|---|---|
| **CIMT Role** | **Assigned Contact (1st, 2nd & 3rd)** | **Contact Details** |
| **Incident Controller (IC)** | **1st:** Chief Property & Facilities Officer<br>**2nd:** PVC People & Culture<br>**3rd:** Director, Health, Safety & Wellbeing | **1st:** Steven Dickson<br>**2nd:** Jane Street<br>**3rd:** Felicia Mudge |
| **Deputy IC (2IC)** | **1st:** PVC People & Culture<br>**2nd:** Director Risk & Assurance | **1st:** Jane Street<br>**2nd:** Joshua Lu |
| **Spokesperson** | **1st:** PVC Engagement & Communication<br>**2nd:** DVC Finance & COO | **1st:** David Harrison<br>**2nd:** Mike Conry |
| **Human Resources Officer** | **1st:** PVC People & Culture<br>**2nd:** Director, Employee Services | **1st:** Jane Street<br>**2nd:** Felicia Mudge |
| **Legal Officer** | **1st:** Principal Legal Counsel<br>**2nd:** Legal Counsel | **1st:** Charbel Haddad<br>**2nd:** Josephine DiFava |
| **Media Officer** | **1st:** PVC Engagement & Communication<br>**2nd:** Communications Advisor | **1st:** David Harrison<br>**2nd:** Breyon Gibbs |
| **Communications Coordinator / Public Information Officer** | **1st:** PVC Engagement & Communication<br>**2nd:** Communications Advisor | **1st:** David Harrison<br>**2nd:** Bryon Gibbs |
| **Student Services Officer** | **1st:** PVC Student Experience<br>**2nd:** Director Student Engagement and | **1st:** Selma Alliex<br>**2nd:** Louise Pollard |

| | | |
|---|---|---|
| | Support | |
| **Finance Officer (Insurance)** | **1st:** Chief Financial Officer<br>**2nd:** Director, General Finance | **1st**: Emily Townsend<br>**2nd**: Sindiso Tshuma |
| **Logistics, Security & Facilities Officer** | **1st:** Director, Facilities & Asset Mgt<br>**2nd:** Deputy Director, Facilities & Asset Mgt | **1st:** Harish Patel<br>**2nd:** Cheryl Swales |
| **Information Services Officer** | **1st:** Chief Information Officer<br>**2nd:** Director IT Service Delivery & Operations | **1st:** Darryl Kefford<br>**2nd:** Sten Christensen |
| **Health Safety & Wellbeing Officer** | **1st:** Director, Health Safety & Wellbeing<br>**2nd:** Senior Advisor, Health Safety & Wellbeing | **1st:** Felicia Mudge<br>**2nd:** Tina McDonald |
| **CIMT Officer** | **1st:** Executive Assistant 1<br>**2nd:** Executive Assistant 2<br>**3rd:** Executive Assistant 3 | **1st:** Tara Lennon<br>**2nd:** Em Jarman<br>3rd: Gheeta Krishnan; |

| CIMT Role | Role Description |
|---|---|
| **Incident Controller (IC)** | Responsible for activating, directing and coordinating the CIMT and their respective activities.<br>Determines whether a critical incident is over and the CIMT should de-escalate. |
| **Deputy IC (2IC)** | ▪ The 2IC is the back up for the IC and is responsible for coordination and decision making if the IC is unavailable.<br>▪ Relieves the IC for incidents with a long duration e.g. to allow the IC to rest<br>▪ Coordinates activities and provides IC support.<br>▪ Assists the IC by considering any actions that have been missed or are overdue |
| **Spokesperson** | ▪ Responsible for communicating to all internal and external stakeholders (focus on media and external stakeholders). |
| **Human Resources Officer** | ▪ Responsible for coordinating temporary staffing, benefits issues, bringing in grief counsellor(s) and other staff support matters. |
| **Legal Officer** | ▪ Responsible for providing legal advice and support to the IC and CIMT where required |
| **Media Officer** | ▪ Responsible for managing media communications (e.g., constructing responses, liaising with legal, etc.) and monitoring media information. |
| **Communications Coordinator / Public Information Officer** | ▪ Responsible for coordinating internal (i.e., the Board, Audit & Risk Committee, and the Vice Chancellor) and external communications – both inbound and outbound. This role focuses on non-media communications. |
| **Student Services Officer** | ▪ Responsible for ensuring students are notified of the University's critical incident processes (including in orientation and, for overseas students, in the pre-departure guide).<br>▪ Responsible for coordinating all student and pastoral related matters, notifying relevant areas of the University (e.g. Student Administration, International Office, Schools, Faculties) and sourcing student related information (e.g. address details, next of kin, etc.).<br>▪ Responsible for ensuring critical incidents involving overseas students are managed in accordance with: *Standard 6: Student Support Services*, and *Standard 5: Younger Overseas Students (in the event students are under the age of 18)* the *National Code of Practice for Providers of Education and Training to Overseas Students 2018.* |

| CIMT Role | Role Description |
|---|---|
| | ▪ Contributing to student communications (working in conjunction with the Communications Coordinator) |
| **Finance Officer (Insurance)** | ▪ Responsible for monitoring and coordinating with suppliers and other commercial contacts – including UNDA's insurance brokers and underwriters where required. |
| **Logistics, Security & Facilities Officer** | ▪ Responsible for managing facilities and security requirements e.g. assessment of building/campus safety, security, or transfer of staff/students to other areas.<br>▪ Primary liaison with Emergency Services where required. |
| **Information Services Officer** | ▪ Provides CIMT with advice on Cyber, IT and communication systems matters.<br>▪ Directs the IT team as it works to restore information systems and networks affected by the incident.<br>▪ Assists in coordinating the telecommunications and IT required for the Command Centre and CIMT mobilisation and operations |
| **Health Safety &Wellbeing Officer** | ▪ Provides CIMT with advice on health, safety and wellbeing matters.<br>▪ Responsible for notifying the WHS Regulator (SafeWork NSW/Worksafe WA/Worksafe VIC) and ensuring the site is preserved when an investigation is required by Inspectors.<br>▪ Provide staff exposed to the critical incident with emotional support, grief and crisis response counselling via EAP. |
| **CIMT Officer** | ▪ Provides administrative support to the CIMT and ensures that action items are recorded and progressed in a timely manner.<br>▪ Directly supports the IC and the 2IC.<br>▪ Assists in coordinating post event debriefs and CIMT training |

# 7 RESPONDING TO THE CRITICAL INCIDENT

## 7.1 Confirm Details & Respond

7.1.1 Once the CIMT is convened it will assume responsibility for the response to the incident. This responsibility continues for as long as the CIMT is convened.

7.1.2 The CIMT will:

- Coordinate Emergency Evacuation procedures (if required).
- Liaise with relevant subject matter specialist staff and relevant parties (such as Emergency Services) to ensure effective ongoing management of the incident and post recovery.
- Notify relevant emergency contacts for staff or students involved in the incident and provide appropriate support. If a staff member or student dies or sustains serious injury, this support may extend to the tasks that may otherwise have been dealt with by family.
- Coordinate appropriate counselling and support services for any staff member or student involved in the Critical incident.

## 7.2 Internal & External Communications

7.2.1 The CIMT, through the Communications Coordinator, manages communication both internally to staff and students and externally through media statements and releases. Internal communication includes notifying and updating key internal stakeholders such as the Board, Audit & Risk Committee, and the Vice Chancellor.

7.2.2 Reporting to and liaising with relevant regulators and authorities, as required.

7.2.3 Communication to any external stakeholders (particularly media) should be conducted through the Spokesperson, with the content of the communication being reviewed and approved by the Media

Officer and IC.

7.2.4 Where a student involved in a critical incident is an overseas student, the Director, Student Engagement and Support is also responsible for ensuring the relevant Faculty and Student Administration and is advised of any leave requirements, to enable Student Administration to record in the Student Management System and report on the Provider Registration and International Student Management System (PRISMS), within 14 days if the oversea student is under the age of 18 and within 31 days for other overseas students.

### 7.3 Critical Incident Monitoring

7.3.1 IC (with the support of the CIMT) is to continuously review and assess how the critical incident is developing. The IC is required to determine and declare if the critical incident can be de-escalated.

7.3.1 De-escalation of the critical incident will transfer responsibility for the incident response from the CIMT to the normal UNDA management structure and localised business process owners. This transfer of responsibility may require input from the Recovery Coordinator to facilitate the transition to procedures required in the *Business Continuity Plan*.

### 7.4 Critical Incident Evaluation

7.4.1 Once the incident has de-escalated from a Critical Incident to a recovery stage the CIMT will arrange a Critical Incident review meeting. At this meeting the CIMT will complete a *Critical Incident Occurrence Report.* Potential matters to be included are listed below:

- Provide a confidential *Critical Incident Occurrence Report* to the Deputy Vice Chancellor, Finance and Vice Chancellor informed by feedback gathered from those present at the incident and other stakeholders. This should include recommendations for the management of such incidents in the future as appropriate.
- Ongoing plans to follow up on the well-being of individuals involved in the incident. This support may be extended to provide accommodations or adjustments to student or staff workload to provide for recovery from injury or shock.
- Ensuring (in conjunction with the Legal Office) that the University complies with any additional legal and/or compliance requirements that may arise from the incident.
- If deemed necessary, the Academic Registrar will contact the Department of Home Affairs and/or the International Student's next of kin to update them further (this may also be done during the incident response).
- Incorporate any learnings from the critical incident to the Critical Incident Management Policy and Procedure.

### 7.5 Training and awareness

7.5.1 The IC has responsibility for coordinating the training of the CIMT and any improvement actions identified from post-incident reviews (refer to 7.4). This includes mock incident response exercises at least once a year.

7.5.2 The Deputy Vice Chancellor Finance & Chief Operating Officer has the responsibility for the update and management of the Critical Incident Management Policy and Procedure.

### 4.1 Maintaining records of Critical Incidents

7.5.3 The Chief Properties and Facilities Officer will maintain a Critical Incident Register and a record of critical incidents, and the remedial action taken, ensuring that:

- confidentiality is maintained in accordance with the *Policy: Privacy*, and

- where the critical incident involves a student of the University, records are retained for at least two years after the student ceases to be an accepted student.

### 7.6 Reporting on critical incident management

7.6.1 Deputy Vice Chancellor Finance & Chief Operating Officer will report annually to the Audit and Risk Committee on the University's management of critical incidents.

# 8 VERSION CONTROL

| Version | Date of approval | Approved by | Amendment |
|---|---|---|---|
| 1 | 29 June 2012 | Vice Chancellor | Effective date – new Policy. |
| 2 | 4 August 2013 | Vice Chancellor | Updated Designated Officer and Contact Details list. |
| 3 | 28 October 2014 | Vice Chancellor | Updated Designated Officer and Contact Details list. |
| 4 | 11 May 2018 | Vice Chancellor | Effective date – new Procedure (procedural information extracted from existing Critical Incident Management Policy). |
| 5 | 27 June 2019 | Senior Operations Officer | Updated to new Procedure template. |
| 6 | 1 July 2019 | COO | Updated Broome contacts. |
| 7 | February 2021 | Vice Chancellor | Updated to reflect the organisational restructure. |
| 8 | 14 December 2022 | Vice Chancellor | Major amendments - updated to align with current organisational structure and university processes, including IT recovery. |
| 9 | 19 April 2023 | Deputy Vice Chancellor, Finance & Chief Operating Officer | Minor amendments to include the definition of a critical incident and record keeping requirements in the National Code 2018. |
| 10 | 30 June 2023 | Chief Property and Facilities Officer | Administrative amendments to contact details. |

## 9 PROCESS SUMMARY

| *Process Step* | *Responsibility* |
|---|---|
| ***First Response – Campus-related Incidents*** | |
| • Immediately contact Security if involved in, witnessing or becoming aware of a potential campus-related Critical Incident. If you feel you are immediately at-risk phone 000, then follow up with security, if possible, who will coordinate with emergency services and attend to the incident. | Relevant staff member |
| • Contact relevant Emergency Services, the University Logistics, Security & Facilities Officer, and the Incident Controller | Security |
| • Attend the location, offer assistance and assist Emergency Services as appropriate | University Logistics, Security & Facilities Officer |
| ***First Response – Student/Staff-related Incidents*** | |
| • Immediately take appropriate action to protect life or protect injury to person, self or others if involved in, witnessing or becoming aware of a potential student/staff-related Critical Incident. If you feel you are immediately at-risk phone 000, then follow up with security if possible, who will coordinate with emergency services and attend to the incident. | Relevant staff member |
| • If appropriate, notify Security. For students, inform the relevant student's Faculty supervisor and/or Pro Vice Chancellor Student Experience. For staff, inform the relevant staff member's supervisor and/or Pro Vice Chancellor People & Culture | Relevant staff member |
| • Contact relevant Emergency Services, the University Logistics, Security & Facilities Officer, and the Incident Controller | Security |
| • Attend the location, offer assistance and assist Emergency Services as appropriate | University Logistics, Security & Facilities Officer |
| • For students: Notify the Manager Student Wellbeing and National Counselling Coordinator to provide appropriate support and or debriefing via the Student Counselling Service | For students: Relevant Faculty supervisor and/or PVC Student Experience |
| • Where the student is an overseas student, notifying the student's parent/s or legal guardian/s, confirming accommodation and welfare arrangements if the student is under 18 years of age. | |
| • For staff: Support and debrief the affected staff member as appropriate | For staff: Relevant staff supervisor and/or PVC People & Culture |
| ***First Response – Cyber-related Incidents*** | |
| • Immediately contact the Notre Dame IT Service Desk if involved in, witnessing or becoming aware of a potential cyber-related Critical Incident | Relevant staff member |
| • Invoke the Cyber Incident Response Plan and report to the Director, IT Business Partners & Security | IT Service Desk |
| • Inform the Incident Controller | Director, IT Business Partners & Security |

| | |
|---|---|
| ***Incident Controller First Actions***<br>• Confirm the incident is to be dealt with as a Critical Incident<br>• Communicate to the DVC Finance & Chief Operating Officer and/or the Vice Chancellor<br>• Control the situation, liaising with the relevant subject matter expert | Incident Controller |

| | |
|---|---|
| ***Critical Incident Management Team***<br>• Convene the Critical Incident Management Team (CIMT) including advising a physical and/or virtual meeting location<br><br>• Take responsibility for the response to the incident. This may include, as appropriate:<br>- Coordination of evacuation procedures<br>- Effective ongoing management of the incident<br>- Managing internal and external communications, including with staff and students, the media and regulators<br>- Informing key internal stakeholders such as the Board and Audit & Risk Committee<br>- Coordinating counselling and support services | Incident Controller<br><br>CIMT |

| | |
|---|---|
| ***Critical Incident Monitoring***<br>• Monitor development of the Critical Incident<br>• Declare de-escalation of the Critical Incident as appropriate | Incident Controller |

| | |
|---|---|
| ***Critical Incident Evaluation (Post De-escalation)***<br>• Provide a confidential Critical Incident Occurrence Report to the DVC Finance & Chief Operating Officer and the Vice Chancellor<br>• Follow-up on the well-being of individuals involved in the incident<br>• Ensure ongoing legislative compliance<br>• Incorporate learnings from the incident to the Critical Incident Management Policy and Procedure | CIMT |