Critical Incident Management procedure

Section 1 - Preamble

(1) This Procedure is effective from 12 January 2021.

Section 2 - Purpose

(2) This Procedure outlines the University's processes to effectively manage critical incidents.

(3) In addition to this Procedure, the Critical Incident Management Plan contains operational instructions and guidance relating to critical incident management at the University.

Section 3 - Scope

(4) This Procedure applies to the management of any critical incident, whether on or off-shore, that has an impact on members of the Deakin community or University activities.

Section 4 - Policy

(5) This Procedure is pursuant to the Critical Incident Management policy.

Section 5 - Procedure

Detecting and reporting a critical incident

(6) Any incident has the potential to start as or escalate into a critical incident. Incident types include, but are not limited to:

a. crisis events such as fire, explosion, chemical spill, gas leak, pandemic, natural disaster, international critical incident, power outage, violent attack, fatality or serious injury.
b. issues or events (internal or external) which may develop into crisis situations, such as health concerns, fraud or mismanagement.
c. seemingly innocuous activities that may attract adverse attention from government, regulators, interest groups, the public or media.

(7) All incidents must be reported to the University's Security Services by calling 222 (internal) or 1800 062 579, if they:

a. cannot be controlled through standard procedures; or
b. threaten or have potential to threaten the Deakin community or the University’s operations, assets or environment.

(8) There are a number of procedures established within the University for the management of incidents, these include:

a. emergencies: the University's Emergency and Crisis Information web page outlines the process for responding to different types of emergencies.
b. security incidents: the security web page outlines the security management arrangements of the University; in addition, the Safer Communities service web page outlines the University's process for responding to concerning, inappropriate or threatening behaviour.
c. travel incidents: the Student International Placements and Programs procedure and the University's Travel policy and Travel procedure outline specific processes in relation to travel related incidents.
d. cyber security incidents: the Information and Communications Technology Security policy outlines the specific process in relation to cyber security.
e. other: there are a number of other standard procedures established within the Faculties and Portfolios of the University for the management of specific incidents that are minor or operational in nature.

Responding to a critical incident

(9) All incidents reported to Security Services are classified as Level 1, 2 or 3 according to the risk-based critical incident classifications outlined in the Critical Incident Management policy.

(10) Level 2 or 3 incidents must be escalated by Security Services in accordance with the Critical Incident Management Plan. This process results in the incident being reviewed and where necessary, directed to the Critical Incident Management Team Leader for formal incident classification.

(11) The Critical Incident Management Team Leader will evaluate the reported incident and where necessary activate the Critical Incident Management Team . Where appropriate the Critical Incident Management Team Leader will consult:

a. advice issued by the government agencies including the Commonwealth Department of Health and the Victorian Department of Health and Human Services
b. travel warnings issued through SmartTraveller, International SOS or the University's approved Travel Consultant
c. advice from international agencies such as the World Health Organisation
d. Faculties and Portfolios of the University to determine the impact of the disaster, emergency or pandemic to the University community and University activities.

(12) The Critical Incident Management Team will refer to the Critical Incident Management Team Leader and provide executive decisions and strategic direction on University priorities when responding to the critical incident.

(13) The Critical Incident Management Team will:

a. seek advice from the General Counsel about any statutory obligations or external reporting obligations arising from a critical incident
b. report any incident involving suspected fraud or corruption to the Chief Financial Officer in accordance with the Fraud and Corruption Prevention and Control policy
c. ensure that stakeholders and regulatory bodies, including but not limited to, the Tertiary Education Quality Standards Agency, WorkSafe Victoria and the University's insurer are notified in a timely manner and provided with appropriate information.

(14) Subject matter experts within the University will be enlisted by the Critical Incident Management Team to:

a. assist with the response as required

b. implement any operational guidelines relating to a specific incident type, e.g. international student incidents, off-shore incidents or world disasters.

(15) Where applicable, costs incurred by a student or student's next of kin or family as a result of a critical incident will be met by the student or the student's family, unless:

a. approval to provide ex gratia financial support has been granted by the Vice-Chancellor; or
b. the General Counsel determines the University has an obligation to provide financial support.

Recovering from a critical incident

(16) The Critical Incident Management Team will design and implement a comprehensive recovery process when the immediate aspects of a critical incident are under control, addressing short and long term issues.

(17) When an incident disrupts a critical activity or process, the University's Business Continuity policy and Business Continuity procedure will be implemented.

Learning and adapting from a critical incident

(18) The University undertakes a process of learning and adapting after critical incidents through debriefs conducted before the Critical Incident Management Team is stood down and a structured post incident debrief and evaluation process according to the scale and impact of the event.

(19) After the debriefing and evaluation program is complete, the Emergency Management Committee oversees a comprehensive follow-up process designed to:

a. provide proper closure for those involved in an incident
b. enable the University to identify lessons learned and implement improvements that reduce vulnerabilities to similar situations in the future.

Planning and preparing for a critical incident

(20) Annual training and testing of the University's critical incident management arrangements will be undertaken, with outcomes reported through the Emergency Management Committee and annual assurance provided to the University Executive.

Accountability

(21) In addition to the accountabilities outlined in the Critical Incident Management policy, the following responsibilities apply to critical incident management:

(22) The Critical Incident Management Team is responsible for providing executive decisions and strategic direction on University priorities when responding to, recovering and learning from critical incidents.

(23) The Emergency Management Committee is responsible for:

a. periodically identifying threat scenarios which are particularly high risk (due to probability and consequence) and developing response guidelines accordingly
b. overseeing an annual internal review to assess the adequacy of Deakin's critical incident management arrangements in light of any changes in the organisation and its operating environment
c. providing strategic direction and identifying opportunities to improve the effectiveness, efficiency and integration of emergency management, risk management, business continuity, ICT recovery and health, wellbeing and safety areas

d. overseeing an annual training and testing program to provide a reasonable level of assurance about the University's critical incident management capabilities, and to enable continuous improvement in relevant arrangements.

(24) The Executive Director, Campus Services is responsible for directing the annual training and testing program for the University's critical incident management arrangements, reporting outcomes through the Emergency Management Committee and providing annual assurance to the University Executive.

(25) The Executive Director, Campus Services will notify the Director, Academic Governance and Standards of critical incidents that will have a significant impact on the University's ability to meet the Higher Education Standards. The Director, Academic Governance and Standards will ensure that the Tertiary Education Quality and Standards (TEQSA) is notified where required under the Tertiary Education Quality and Standards Agency Act 2011.

(26) The Executive Director, Human Resources will notify the Director, Academic Governance and Standards of material breaches in safety that will have a significant impact on the University's ability to meet the Higher Education Standards. The Director, Academic Governance and Standards will ensure that the Tertiary Education Quality and Standards (TEQSA) is notified where required under the Tertiary Education Quality and Standards Agency Act 2011.

(27) The Executive Director, Human Resources is responsible for providing subject matter expertise and incident response relating to health, wellbeing, safety and local emergency arrangements.

(28) The Executive Director, Student Life is responsible for providing subject matter expertise for critical incident response relating to all students.

(29) The Senior Manager, Global Mobility is responsible for providing subject matter expertise in responding to international critical incidents involving members of the Deakin community engaged in approved international mobility programs.

(30) Security Services are responsible for establishing and implementing the annual training and testing program for the University's critical incident management arrangements and the establishment and maintenance of systems to detect, respond and report to critical incidents.

(31) The Director, Security, Transport and Retail is responsible for reporting significant travel warnings and advice relating to staff travel arranged through the University's approved Travel Consultant.

(32) The affected Faculty or Portfolio, in conjunction with the Critical Incident Management Team, is responsible for the identification of staff and students who are affected or traumatised as a consequence of a critical incident and for ensuring that appropriate communication and support is offered.

(33) All University staff, and where appropriate non-staff members of the Deakin community, must ensure that all incidents are reported as per clause 8 of this Procedure.

(34) All University staff with management and supervisory responsibilities must ensure that any procedures established for the management of area specific incidents include appropriate reporting and escalation elements that satisfy clause 8 of this Procedure.

Section 6 - Definitions

(35) For the purpose of this Procedure:

a. pandemic: an epidemic of infectious disease that has spread across a wide geographic area and affected human populations across a large region i.e. a whole region or continent.

Status and Details

Status	Current
Effective Date	12th January 2021
Review Date	5th February 2021
Approval Authority	Council Secretary
Approval Date	12th January 2021
Expiry Date	To Be Advised
Responsible Executive	Kean Selway Chief Operating Officer chiefoperatingofficer@deakin.edu.au
Implementation Officer	Chris Jones Executive Director, Campus Services +61 3 52271246
Enquiries Contact	Campus Services +61 3 52271246