Critical Incident Management policy

Section 1 - Preamble

(1) This Policy is effective from 19 June 2017.

Section 2 - Purpose

(2) This Policy outlines the University's commitment to effectively managing critical incidents.

Section 3 - Scope

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

Section 4 - Policy

(4) The University is committed to ensuring that an effective critical incident management processes, aligned with the Australasian Inter-Service Incident Management System (AIIMS) model is implemented across the University to:

a. protect the University's employees, students, associates, and other stakeholders such as partners, neighbours and visitors to Deakin campuses and events
b. protect the University’s assets and environment
c. ensure continuity of the University's critical business activities
d. protect the University's reputation.

(5) The University's critical incident management capability is designed and implemented around 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
e. learning and adapting - reviewing and improving arrangements.

(6) The University will establish and maintain an Emergency Management Committee chaired by the Chief Operating Officer.

(7) The role of the Emergency Management Committee is to oversee the University’s emergency management system above and beyond any particular critical incident. This includes:

a. all emergency management planning and preparation
b. training
c. review and compliance.

(8) The University will use a risk-based critical incident classification and escalation process in alignment with the University's Risk Assessment Matrix.

a. 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
    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. A 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
    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. A 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
    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.

(9) The University will maintain a Critical Incident Management Plan and a trained and competent Critical Incident Management Team to control the University's strategic response and provide executive decisions and strategic direction relating to a critical incident.

(10) The University will undertake an annual internal review of the Critical Incident Management Plan and complete annual training and testing of the University's Critical Incident Management Team and associated systems or capabilities.

Accountability

(11) Designated senior staff members of the University are responsible for the strategic direction, development, implementation, management and validation of capabilities and functions to manage critical incidents, specifically:

a. the Chief Operating Officer is the University’s Critical Incident Coordinator and is responsible for adequately resourcing the critical incident management program for the University.
b. the Executive Director, Campus Services is responsible for the Critical Incident Management Plan, Critical Incident Management Team, Emergency Management Committee, Security Services and systems, critical incident training, testing and compliance.
c. the Executive Director, Human Resources is responsible for the health, wellbeing and safety procedures relating to staff including local emergency arrangements.
d. the Executive Director, Student Life is responsible for the health, wellbeing and safety procedures relating to students including the Threat Assessment Management Team, Safer Community Service and where relevant compliance with the Education Services for Overseas Students Act 2000 (Cth).

e. the Deputy Vice-Chancellor Global Engagement is responsible for incident management and emergency procedures relating to members of the Deakin community engaged in approved international mobility programs.
f. the Chief Digital Officer is responsible for Information and Communication Technology (ICT) incident management procedures.

Section 5 - Procedure

(12) The Critical Incident Management procedure documents how to comply with this Policy.

Section 6 - Definitions

(13) For the purpose of this Policy:

a. business continuity: capability of the organisation to continue delivery or products or services at acceptable predefined levels following a disruptive incident.
b. critical incident: a high consequence event or series of events that threatens or has potential to threaten the Deakin community or the University’s operations, assets, environment and requires urgent attention.
c. Critical Incident Management Plan: a plan that describes the University's critical incident management arrangements.
d. Critical Incident Management Team: the team responsible for providing executive decisions and strategic direction on University priorities when responding to critical incidents.
e. Deakin community: includes students and staff as well as members of the general community who use facilities or are affected by the operations of the University. For the purpose of Critical Incident Management, the Deakin Community also includes external organisations whilst operating on University property.
f. University activities: all activities, both on and off-shore, undertaken by Staff, Students or the Deakin Community within the management and control of the University.
g. University property: all land, buildings, other property and facilities owned by, under the control of or occupied by the University.

Status and Details

Status	Current
Effective Date	19th June 2017
Review Date	19th June 2020
Approval Authority	University Council
Approval Date	19th June 2017
Expiry Date	To Be Advised
Responsible Executive	Kean Selway Chief Operating Officer +61 3 52278588
Implementation Officer	Chris Jones Executive Director, Campus Services +61 3 52271246
Enquiries Contact	Campus Services +61 3 52271246

This policy 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 Policy Library for the latest version.