Critical Incident Management Policy

Section 1 - Background and Purpose

(1) The Policy covers the incident response and disruption management planning and process requirements for all campuses, Divisions, Colleges, Schools and Divisions of the University. Specific policy requirements for the disaster recovery of IT systems and infrastructure are outside of the scope of this Policy.

Preamble

(2) The Procedure covers the requirements for incident response and disruption management planning and procedural requirements for all campuses, Divisions, Colleges, Schools, Divisions and Institutes of the University.

General

(3) The principles of these procedures are that:

a. Key internal stakeholders are aware of the need to respond appropriately to incidents and to manage any resulting disruption that may occur;
b. Resources and processes are made available and capable to ensure the continued achievement of the University key objectives following a critical incident;
c. Staff are familiar with and trained in their roles under the Critical Incident Management Plan.

Section 2 - Scope

(4) Applies to:

a. All campuses of the university;
b. All staff, students, Council members, volunteers and contractors;
c. All activities that are under the control or direction of the University, whether conducted on or off university property.

Section 3 - Policy Statement

(5) The aim of the Critical Incident Management Policy is to provide a framework for the response to and management of critical incidents.

(6) Such incidents encompass those that significantly threaten the safety and security of University staff, students, contractors, guests, or visitors; the ongoing performance of the University's critical business functions; or result in significant adverse impacts on the local community arising from University activities.

Section 4 - Procedure

Framework for Critical Incident Management

(7) The framework is based upon planning and preparedness for the three prime responses following any critical incident:

a. Emergency response: providing a capability to manage the immediate issues arising from the incident and focusing on the protection of life and property;
b. Business continuity phase: providing a capability to assist the University to continue to operate its critical business functions; and
c. Recovery phase: restoring critical business function and infrastructure to a state of routine operation.

Annual Critical Incident Management Cycle requirements

(8) The annual Critical Incident Management Cycle is coordinated by the Risk Management Division and comprises:

a. Identification and confirmation of key risks contributing to potential critical incidents;
b. Ensuring specific emergency responses are in place to manage each critical incident;
c. Confirming responsibilities and accountabilities of members of each of the defined response teams;
d. Ensuring that a Critical Incident Management Plan is maintained;
e. Conduct of a business impact analysis covering the University's critical business functions;
f. Development and maintenance of Business Continuity Plans (BCPs) providing coverage for each of the University's critical business functions; and
g. Review and exercising of plans on an annual basis.

Command Roles

(9) Governance, control and coordination of critical incident management are vested in a hierarchy of response teams, comprising:

a. Critical Incident Management Team, established at a 'Gold' (whole of University), 'Silver' (central Bundoora campus command), or 'Bronze' level (local command at any other campus), with responsibilities for the overall management and oversight of all plans and responses;
b. Emergency Response Team, established at each campus with responsibility for the activation and management of the Emergency Response Plan;
c. Recovery Team, to be established for coordinating the recovery and restoration activities (composition will be dependant upon the nature of the specific recovery requirements); and
d. Business Continuity Teams, established at College and Division level to manage the implementation of BCPs.

Governance Responsibilities

(10) Corporate Governance, Audit and Risk Committee (CGARC) will approve annually the most current version of the Critical Incident Management Plan. An annual report will be prepared for CGARC providing a review of the current critical incident management capability across the University. Such examination will be based upon a combination of assurance review and exercising of plans and capability.

Senior Management Responsibilities

(11) Each senior manager, for their respective areas of responsibility, will annually:

a. Confirm which of its functions constitute a critical business function;
b. Determine the currency of existing Plans and identify the need for new Plans to be developed;
c. Nominate a responsible person (BCP Coordinator) that will be tasked with preparing and maintaining Plans to meet local requirements;
d. Provide to CGARC, through Risk Services, certification (with such caveats as necessary) to the status of their preparedness.

Risk Management Unit Responsibilities

(12) To:

a. Co-ordinate the establishment and maintenance of the Critical Incident Management Framework;
b. Facilitate governance reporting to CGARC;
c. Provide advice on preparedness and response to the University community.

Internal Audit Responsibilities

(13) Internal Audit will conduct regular reviews of pertinent aspects of the Critical Incident Management Framework as deemed necessary and approved by Corporate Governance, Audit and Risk Committee.

Section 5 - Definitions

(14) For the purpose of this Policy and Procedure:

a. Critical incident: A situation where the University (or parts thereof) shift from routine to non-routine operation, in response to an actual or potential incident with high consequences. This is usually typified by the area affected requiring additional (centralised) assistance in its management
b. Emergency: An event, actual or imminent, which endangers or threatens to endanger life, property or the environment, and which requires a timely and coordinated response.

Section 6 - Stakeholders

Responsibility for implementation – Critical Incident Management Team; Threat Assessment Team; Emergency Management Team; Emergency Planning Committee.

Responsibility for monitoring implementation and compliance – Corporate Governance, Audit and Risk Committee.

Status and Details

Status	Current
Effective Date	15th November 2016
Review Date	1st August 2018
Approval Authority	University Council
Approval Date	15th November 2016
Expiry Date	Not Applicable
Unit Head	Natalie MacDonald Vice-President (Strategy and Development) +61 3 9479 1862
Author	Vanessa Cover Director, Risk Management
Enquiries Contact	Stacey Conlin Director, Risk Management