



# Business Continuity policy

## Section 1 - Preamble

(1) This Policy is effective from 22 February 2018.

## Section 2 - Purpose

(2) This Policy sets out the guiding principles under which Business Continuity is to be developed, implemented and managed to enable the University to establish and maintain an effective level of preparedness to respond to incidents that disrupt normal operations.

## Section 3 - Scope

(3) This Policy applies across the University.

## Section 4 - Policy

(4) The University is committed to ensuring that an effective business continuity management (BCM) program is implemented to minimise the disruption of activities due to the unavailability of 'business as usual' resources, for example but not limited to:

- a. facilities, e.g. flood, fire, power outage, chemical spill, denial of access
- b. people, e.g. pandemic/epidemic, industrial action, extreme flu season
- c. vital records, e.g. electronic and hard copy records
- d. information and communications technology (ICT), e.g. computer hardware, applications and telecommunications
- e. equipment, e.g. cold rooms, research equipment, desks and chairs
- f. externally provided service or resource e.g. contractors, software vendors.

(5) BCM requirements will be assessed via a Business Impact Analysis (BIA) for activities undertaken by all Faculties and Portfolios. Impacts will be assessed in accordance with the Risk Management policy [Schedule A: Risk Matrix](#).

(6) Activities assessed as having a recovery time objective of 15 days or less are deemed critical activities. Recovery steps for these activities and their associated resources will be included in the University's Business Continuity Plan (BCP).

(7) Continuity of service provision must be adequately addressed for services, infrastructure, and/or any resources provided by an external party via certification arrangements, service level agreements and/or other contractual arrangements appropriate to the assessed level of risk.

## Accountability

(8) The University Executive will demonstrate a high level of commitment to this Policy and support a culture aimed at building organisational resilience through the implementation and continued improvement of preparedness and response capabilities.

(9) The Executive Director, Campus Operations, is responsible for centrally coordinating the BCM program.

(10) The Emergency Management Committee will provide strategic direction and oversight for BCM in accordance with the [Critical Incident Management procedure](#).

(11) The Critical Incident Management Team will provide executive decisions and strategic direction on University priorities when responding to critical incidents affecting the University and managing related Business Continuity responses.

(12) Directors (or equivalent) and Faculty General Managers are the custodians of BCM capability within their area. Supported by Campus Services, they are responsible for the development, maintenance and validation of their specific BCP information (found within the Deakin University BCP), the management of any risks relating to BCM in accordance with the University's [Risk Management policy](#) and the instigation of a BIA for new or changed activities within their areas.

(13) The Chief Information and Digital Officer, is responsible for ICT continuity and disaster recovery processes including the alignment of ICT service levels and disaster recovery priority groups with the BIA.

## Section 5 - Procedures

(14) The [Business Continuity procedure](#) documents how to comply with this Policy.

## Section 6 - Definitions

(15) For the purpose of this Policy:

- a. Activity: process or set of processes undertaken by the University (or on its behalf) that produces or supports one or more products or services.
- b. Business Continuity Management (BCM): capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.
- c. Business Continuity Plan (BCP): a document to be referred to by the affected Faculty or Portfolio during a disruptive incident that outlines the steps required to recover.
- d. BCM Program: ongoing management and governance process supported by the University Executive and appropriately resourced to implement and maintain Business Continuity management.
- e. Business Impact Analysis (BIA): process of analysing activities and the effect that a business disruption might have upon them.
- f. Recovery Time Objective: the period of time following an incident within which an activity must be resumed, or resources must be recovered.

## Status and Details

<b>Status</b>	Current
<b>Effective Date</b>	22nd February 2018
<b>Review Date</b>	22nd February 2021
<b>Approval Authority</b>	Vice-Chancellor
<b>Approval Date</b>	21st February 2018
<b>Expiry Date</b>	To Be Advised
<b>Responsible Executive</b>	Kean Selway Chief Operating Officer evpfutures@deakin.edu.au
<b>Implementation Officer</b>	Chris Jones Executive Director, Campus Operations
<b>Enquiries Contact</b>	Campus Operations +61 3 52271246