Business Continuity procedure

Section 1 - Preamble

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

Section 2 - Purpose

(2) This Procedure explains how to comply with the Business Continuity policy.

Section 3 - Scope

(3) This Procedure applies across the University.

Section 4 - Policy

(4) This Procedure is pursuant to the Business Continuity policy.

Section 5 - Procedures

Activating a Business Continuity response

(5) Activation of a Business Continuity Management (BCM) response is initiated by the Critical Incident Management Team (CIMT) Leader when an incident disrupts the business as usual operations of the University, and the disruption has or threatens to breach the Recovery Time Objective (RTO) of one or more critical activities.

(6) During a Critical Incident the CIMT has responsibility for BCM and will establish a Business Recovery Team (BRT) who is responsible for coordinating the implementation of the Deakin University Business Continuity Plan (BCP) by the local areas.

(7) To support a large relocation of activities or staff, the CIMT may require the displacement of other areas who are undertaking activities that, through the Business Impact Analysis (BIA) information, are deemed non-time critical in order to access their resources. This may be required to obtain office space or equipment such as computers.

(8) When the situation has been recovered to the point that the CIMT is stood down, the BRT may continue to work with the effected areas and report to the Critical Incident Management Team Leader.

(9) Disruptive incidents that do not require a CIMT response, are managed through implementing the relevant section of the University's BCP by the local area. In these instances, the BRT may provide support.

ICT disaster recovery

(10) ICT disaster recovery is a component of the University's overall business continuity capability. It provides for the timely recovery and restoration of ICT systems and processes, including applications, infrastructure and data

resources that support critical activities.

(11) ICT Recovery is managed in accordance with the Business Continuity policy and the Digital Services ICT Recovery Framework.

Business Continuity Program elements

Policy and Governance

(12) The Business Continuity policy outlines the scope and overarching responsibilities in relation to the management of the University's BCM Program.

(13) The University's BCM program aligns with the international standard ISO 22301:2012 Societal security — Business Continuity management systems, Technical Specification ISO/TS 22317:2015 Guidelines for Business Impact Analysis and the Business Continuity Institute Good Practice Guidelines.

Analysis

(14) A Business Impact Analysis (BIA) is the primary information collection and assessment tool in the development of BCM strategies and plans.

(15) The BIA identifies activities performed and measures the impact of a disruption by assessing the impact over time, determining the service level timing and the maximum tolerable period of disruption.

(16) A Recovery Time Objective (RTO) for each activity is drafted and where these meet the scope of the Business Continuity policy, the dependencies and supporting resources are subsequently identified. Activities captured in this step are deemed critical activities.

Design

(17) The information captured and assessed via the BIA process is used to prioritise the restoration of critical activities and set a suitable RTO within the context of broader university activities. Continuity and recovery strategies are then designed to meet the RTO for these activities.

(18) Where these strategies involve ICT requirements, details will be provided to Digital Services for inclusion and consideration in ICT Recovery analysis and planning.

Implementation

(19) The strategies that have been developed at the design stage are documented within the University's BCP, providing a pre-defined and approved course of action to be initiated in response to an operational disruption.

Validation

(20) Validation of the University's BCM capability is completed annually within the CIMT exercise and periodically through BIA updates, desk checks and simulations. Refer to Table A – Business Continuity Management Validation for more information.

(21) The testing of the University's ICT disaster recovery capability is managed independently by Digital Services.

(22) Risks that are identified from the Business Continuity validation program will be evaluated and treated in accordance with the University's Risk Management policy.

Table A – Business Continuity Management Validation

Level	Scope and Process	Participants	Frequency	Complexity
1 – BIA update	Review and challenge the content of the BIA, including recovery timings and impact scores.	- Campus Services - Local Area staff members - Author of the relevant business continuity plan content	HIGH	LOW
2 – BCP Desk Check	Review and challenge the content of the BCM plan. Check documentation for completeness and accuracy.	- Campus Services - Local Area staff members - Author of the relevant business continuity plan content	MEDIUM	MEDIUM
3 – BCP Simulation	A simulation of a Business Continuity event (disruption)with a response that incorporates one or more of the following: - relocation - workarounds - ICT recovery - Critical Incident Management - emergency response - recovery of third party suppliers.	- Local Area staff members - Business Recovery Team members - Observers - CIMT members - External consultants/facilitator - Campus Services - Author of the relevant business continuity plan content	MEDIUM	MEDIUM
4 – Critical Incident Management Team exercise	BCM procedures are enacted within a Critical Incident Management Team exercise without effective live or production environment.	- Local Area staff members - Business Recovery Team members - Observers - CIMT members - External consultants/facilitator - Campus Services - Author of the relevant business continuity plan content	LOW	HIGH

Accountability and Responsibilities

(23) In addition to the accountabilities listed in the Business Continuity policy, the following shall apply:

a. the CIMT provides executive decisions and strategic direction on University priorities when responding to critical incidents and managing related Business Continuity responses, and:
    i. directs the BRT during a Business Continuity response
    ii. endorses financial decisions relating to the Business Continuity response that are outside of normal delegations
    iii. prepares all communications to relevant stakeholders during the Business Continuity response.
b. the BRT is made up of subject matter experts in Business Continuity, ICT, Timetabling and Facilities Services, and:
    i. reports to the Planning Team of the CIMT or the CIMT Leader during a Business Continuity response
    ii. coordinates the implementation of the Deakin University BCP by local areas when an incident has caused a disruption to a critical activity.

Section 6 - Definitions

(24) Definitions relevant to this Procedure are listed in the Business Continuity policy.

Status and Details

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