Business Continuity Policy

Section 1 - Purpose

(1) Australian Catholic University (ACU) is committed to enabling the timely recovery of its critical business activities and systems in the event of a serious Incident. The Business Continuity Policy has been developed to support recovery and provide guidance to the implementation of Business Continuity Plans (BCP) across the University.

Section 2 - Scope

(2) This Policy describes the actions required to respond to and recover time-critical business activities following a serious Incident impacting ACU's ability to continue its operations.

(3) An Incident is considered serious when it cannot be managed via business-as-usual arrangements, and the Incident has affected (or has the potential to affect):

a. day-to-day operations;
b. the health and safety of staff, students, contractors or visitors;
c. critical governance, legal or regulatory compliance obligations including compliance with the Higher Education Standards Framework (Threshold Standards) 2021; and/or
d. the reputation of the University and/or the community.

(4) This Policy applies to staff, students, contractors, volunteers and visitors while they are participating in university-related activities, both on and off campus, within Australia or overseas.

(5) No part of this Policy overrides the Delegations of Authority Policy and Register, the Code of Conduct for Staff or the Student Conduct Policy.

(6) This Policy and its related resources demonstrate the ACU's commitment to:

a. identifying, managing and preventing major business disruption in line with the Critical Incident Management Policy and BCP; ACU Mission, Identity and Values, governance, legal and reporting regulatory compliance obligations and Enterprise Risk Management Framework and principles;
b. evaluating the effectiveness and adequacy of its Business Continuity response and processes;
c. managing its recovery by the effective implementation of ACU's Business Recovery Plan (BRP); and
d. providing a high level of stakeholder assurance in ACU's recovery capability.

Section 3 - Principles

(7) Business continuity is capability of an organisation to continue delivery of products or services within acceptable time frames at predefined capacity during a serious Incident or emergency.

(8) In the event of an Incident or Critical Incident, ACU can implement business continuity and recovery management measures.

(9) ACU will develop and maintain a Business Continuity Plan (BCP).

(10) The Deputy Vice-Chancellor (Corporate) is responsible for approving the initiation of the Business Continuity Plan (BCP).

(11) Initiation of the BCP will include consultation and on-going engagement with members of the Vice-Chancellor's Advisory Committee during the activation of business continuity and throughout recovery management measures.

(12) The purpose of the BCP is to:

a. provide a structured approach to recovering from a serious Incident;
b. identify the essential operational elements (including interdependencies), staff, systems and resources required to be maintained in the event of a serious Incident; and
c. minimise/control potential impacts of threats on business operations and systems.

(13) ACU's business continuity objectives are to minimise:

a. the impact on people, including staff, students and members of the community;
b. potential safety issues in a non-standard operating environment;
c. disruption to operations and continuity of services;
d. impacts to community wellbeing, financial, educational, reputational, and strategic priorities; and
e. governance, legal and regulatory compliance risks.

(14) ACU's business resilience is integrated on various levels with frameworks across the university to promote an effective and holistic response to serious Incidents, including:

a. Risk Management;
b. Emergency Management;
c. Critical Incident Management;
d. Business Continuity Management;
e. Business Recovery Management;
f. IT Incident Management Process (which includes the IT Major Incident process).

Section 4 - Definitions

(15) In the context of this policy the following terms apply:

Term	Definition
Business Continuity	The capability of the University to continue delivery of products or services within acceptable time frames at predefined capacity during a serious Incident or emergency.
Business Continuity Plan (BCP)	Documented procedures guiding the Critical Incident Response Group (CIRG) and Business Recovery Lead in how to recover, resume, and restore to a pre-defined level of operation for whole of university following a serious Incident.
Business Continuity Management	A holistic management program that identifies serious Incidents and provides a framework for an organisation to provide an effective response that safeguards the interests of its people, property and reputation.
Business Impact Assessment (BIA)	Documented identification of key internal systems, responsible staff, required equipment as well as allowable outage and recoverable time frames of all critical business processes across the University.

Term	Definition
Business Process Owner	Role responsible for managing and overseeing the objectives and performance of a process through Key Performance Indicators (KPI). A process owner has the authority to make required changes related to achieving process objectives.
Business Recovery Lead	Role responsible for working within an organisational unit to recover critical business functions.
Business Recovery Plan (BRP)	Portfolio specific guidelines and template for use by the Senior Executive members in how to recover, resume and restore to a pre-defined level of operation.
Critical Business Functions	Vital functions, without which the university cannot effectively operate and as a result could suffer serious reputation, financial, governance, legal or regulatory compliance risks or other damages or penalties.
Critical Incident	A serious Incident or emergency situation that will or may have the potential to significantly impact the university's business viability, threaten the lives of employees or others, and/or jeopardise the university's reputation.
Critical Incident Management	Process that identifies potential risks to an organisation and provides a framework for establishing resilience to ensure the University can respond effectively to Incidents and Critical Incidents and reduce impact to people, property, finances, reputation or operational or strategic goals. This is achieved by formulating and implementing viable recovery strategies, initiating the CIRG and providing comprehensive training, testing and maintenance programs.
Critical Incident Response Group (CIRG)	The CIRG includes Incident Conveners and other officers of the University who can provide their expertise, resources and support to the Critical Incident Convener while managing a Critical Incident.
IT Incident Management Process	The document outlining the process for recovering ACU's business IT systems.
Emergency Management	Managing risks and undertaking actions to prepare for, prevent and respond to a serious Incident or emergency situation.
Incident	A moderate issue that can interrupt business processes sufficiently to threaten the viability of the university or the welfare of an individual or individuals.
Maximum Allowable Outage	The amount of time a business process can be disrupted without causing significant harm to the organisation.
Recovery Strategy	The approach used by the university to ensure its recovery and continuity in the face of an Incident or Critical Incident.
Resources	All assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that the university requires to operate and meet its objectives.
Risk Management	Documented potential risks to the university, and the steps that should be taken to keep those risks at acceptable levels.

Section 5 - Business Continuity Plan (BCP)

(16) The Business Continuity Plan has been developed to support the continuation and timely recovery of ACU's own critical business activities and systems should an Incident or Critical Incident occur.

(17) The initial focus of Business Continuity is to continue performing Critical Business Functions to maintain the viability of ACU. ACU implements and maintains a holistic approach to Business Continuity which is appropriate to the nature and scale of its operations.

(18) The BCP identifies and determines how continuity and recovery from a serious Incident will be achieved.

(19) Operational units must determine an appropriate Business Continuity strategy for each critical business process and document this in their Business Recovery Plan. Key inputs include the results of a Business Impact Assessment

(BIA) process, a threat assessment outlining credible disruption scenarios, and agreed response structures and strategies.

(20) The BCP outlines the key phases of a serious Incident and the steps required to manage the situation.

a. Phase 1: Identifying and stabilising the situation - A protocol for stabilising the situation when a serious incident occurs. It includes a list of immediate actions that should be performed by ACU personnel, incident assessment tools, contact lists, key roles and responsibilities.
b. Phase 2: Recovering Critical Business Functions - A series of strategies designed to enable the recovery of Critical Business Functions immediately following a serious Incident.
c. Phase 3: Implementing business resumption - A guide to assist the Business Recovery Lead in moving ACU to an operating state that existed prior to the serious Incident.

(21) The BCP may be activated in conjunction with related processes (such as Emergency Management, Incident Management, IT Incident Management Process) as well as Business Continuity Plans of key suppliers.

(22) The BCP may be activated in response to a serious Incident or emergency. The BCP details the activation procedures including when, how and who is responsible for the activation. The BCP may be activated through the Critical Incident Management process, managed by the Critical Incident Response Group (CIRG).

(23) The Critical Incident Convener has responsibility for the management of Business Continuity at the University as outlined in this Policy and its associated documentation.

(24) The decision to activate the BCP sits with the Critical Incident Convener. Activation of the BCP will involve notification to each member of the CIRG.

(25) Once a Critical Incident has been declared, a Business Recovery Lead may be appointed to assess operational impacts on Critical Business Functions resulting from the Critical Incident and to activate the Business Continuity Plan. In doing so, they must continue to follow all instructions from the Critical Incident Convener and CIRG.

(26) Following a serious Incident affecting Critical Business Functions, the Business Recovery Lead will manage the recovery of Critical Business Functions in accordance with the BCP and BRP.

(27) The Business Recovery Lead is responsible for working with organisational units to recover Critical Business Functions. They will report to the CIRG and the Critical Incident Convener.

(28) The Business Continuity arrangements are documented in the BCP and will be managed by the Business Recovery Lead and/or the CIRG.

Section 6 - Business Recovery Plan (BRP)

(29) The Business Recovery Plan supports ACU's BCP and is to be used as a guide and template to facilitate the restoration of business operations after a serious Incident.

(30) The BRP exists for each Portfolio of ACU and documents the priorities, recovery procedures, responsibilities and processes that will support ACU in managing recovery from a serious Incident or Critical Incident.

(31) Key inputs include the results of the BIA process, response to BCPs, and recovery budget management.

(32) The BIA comprises a set of steps to determine and identify Critical Business Functions, key internal resources and systems, and assess the impact of disruption. It sets allowable outage and consistent recovery timeframes and levels to ensure appropriate strategies and business continuity practices are in place for all Critical Business Functions within

ACU.

(33) Each Critical Business Function is assessed on its frequency, business operating period, and maximum allowable outage (MAO). Critical dependencies, impacts and risk levels are identified, and a recoverable time objective is agreed.

(34) Following a serious Incident affecting a Portfolio, personnel will be expected to manage the recovery of Critical Business Functions as per their BRP.

(35) If the serious Incident is at a Portfolio level, the BRP will be activated by the appropriate Senior Executive member.

(36) If the serious Incident is University wide the Business Recovery Lead will liaise with each Portfolio to activate their BRP.

Section 7 - Governance and Review

(37) Business Continuity Plan (BCPs), Business Impact Assessment (BIAs) and Business Recovery Plan (BRPs) must be reviewed by the respective business process owner annually to ensure the contents are accurate, complete, current and relevant.

(38) Each business unit should aim to continually improve the suitability, adequacy or effectiveness of their BIA and BRP.

(39) Post Incident Reviews (PIR) and debriefs should be completed following a serious Incident to learn from what worked and what did not work, and update documentation and training programs to continuously improve. Debriefs and the PIR should involve:

a. key employees;
b. other organisational units; and
c. relevant stakeholders (within Portfolios).

(40) The BCP and BRP will undergo an annual review to ensure accuracy, currency and effectiveness.

Section 8 - Communications / Training

(41) The CIRG meets monthly to engage in discussion about ongoing or recently concluded Incidents and Critical Incidents including:

a. review of the PIR;
b. consideration of the effectiveness of the management of Incidents and Critical Incidents; and
c. options for continuous improvement.

(42) Ongoing support is available to business process owners and is provided by the Program Officer, Strategic Programs. The Program Officer, Strategic Programs is available to provide guidance during review periods and throughout the year as required.

(43) Induction training is provided for new staff and annual scenario training is coordinated by the Program Officer, Strategic Programs.

(44) All communication strategies related to Business Continuity management shall be overseen by the Strategic

Communications team and approved by the Critical Incident Convener.

Section 9 - Associated Information

(45) For related legislation, policies, procedures and guidelines and any supporting resources please refer to the Associated Information tab.

Status and Details

Status	Current
Effective Date	10th May 2024
Review Date	10th May 2029
Approval Authority	Vice-Chancellor and President
Approval Date	10th May 2024
Expiry Date	Not Applicable
Responsible Executive	Patrick Woods Deputy Vice-Chancellor (Corporate)
Responsible Manager	Paul Campbell Deputy Chief Operating Officer
Enquiries Contact	Gillian Rowlands Program Manager, Strategic Programs Office of the Deputy Chief Operating Officer