Information Technology Disaster Recovery Policy

Section 1 - Purpose

(1) This Policy specifies the principles by which Macquarie University and its controlled entities (the University) will ensure appropriate Information Technology (IT) resilience and maintain the delivery of IT services to the University at pre-defined levels, in the event of major disruption, emergency, or disaster.

(2) This Policy supports the broader IT Disaster Recovery Framework of the University and its Controlled Entities.

Scope

(3) This Policy applies to all users of University IT resources and connected systems. This includes:

a. all professional, academic, and research staff, all staff of controlled entities, and all contractors, across all campuses and locations of the University;
b. all organisational and business units, faculties, departments, and divisions, regardless of their location, which must consider how this Policy factors into their operations and service delivery commitments; and
c. all legal entities, suppliers, and vendors working on or supplying the University with IT services who are bound by this Policy as it relates to IT recovery and data loss recovery timeframes.

Section 2 - Policy

(4) Disaster events may be isolated, short term disruptions to service continuity where there is a requirement to activate only the IT Disaster Recovery (IT DR) plan of a single system, or may involve a wider disruption, where the University may need to activate its full Business Continuity Plan (BCP). In all cases, IT DR will be guided by the priorities of the BCP.

(5) The IT DR Framework will be aligned with the University's business continuity processes, risk management approach and Cyber Security Policy. This will be achieved by:

a. ensuring that any IT DR focused business impact analysis identifies the following for each individual application/service to properly quantify and categorise its business recovery requirements:
    i. Maximum Allowable Outage (MAO);
    ii. Recovery Time Objective (RTO);
    iii. Recovery Point Objective (RPO);
b. ensuring that any new University IT systems and applications developed or procured, including associated infrastructure, include new/amended IT DR plans during the system implementation life cycle. New/amended applications will not be released to production without the necessary plan updates, and approval;
c. ensuring that appropriate data protection strategies such as backups, replication, and supplier contractual agreements are in place, to maintain the integrity of the University data, and to prevent or minimise data loss within any identified RPO;
d. requiring that all IT projects or system enhancements comply with the IT DR Policy and Framework including classification of new systems into the organisation's IT DR tiers;

e. requiring that contracts for IT services provided by vendors/suppliers include assurances for IT DR including detailing system recovery times and potential data loss;
f. producing evidence of IT DR plans and regular testing of plans;
g. ensuring that IT DR is implemented and managed in accordance with the processes and procedures set out in the University's IT DR Framework; and
h. undertaking a risk-based approach to all IT DR activities and phases of event management (Response, Recovery, Resumption and Restoration).

IT Disaster Recovery Objectives

(6) The objectives of IT DR are to:

a. manage risk;
b. minimise the impact on the University's operations of disruptions affecting IT services by having in place effective responses, including IT incident management and IT disaster recovery plans;
c. support the University's service level commitments so that IT systems underpinning services and/or time critical functions are recovered as a priority;
d. ensure that all users of University IT resources and connected systems suppliers, and vendors are competent and familiar with their responsibilities and delivery of IT DR;
e. provide evidence-based criteria on which to develop the IT DR strategies;
f. implement a continuous improvement process aligned with business continuity; and
g. align IT DR with relevant University policy, procedures, and guidelines.

(7) IT DR is informed by the following high-level management processes which facilitate the delivery of an integrated University IT DR Framework:

a. Business Continuity Management;
b. Risk Management;
c. IT Service Continuity;
d. Information Security Management; and
e. Asset/Supplier/Vendor Management.

(8) The IT DR Framework aligns with ISO/IEC 27031:2011 IT Security Techniques - Guidelines for IT Readiness for Business Continuity and NSW Disaster Recovery Guidelines (refer Associated Information).

(9) The University through the Chief Information and Digital Officer (CIDO) portfolio will:

a. define an IT DR Framework and develop IT DR Strategies;
    i. ensure that the IT DR Framework follows industry best practice, including relevant national and international standards and guidelines;
b. ensure that IT DR plans to support the University's business recovery requirements are developed, reviewed, and maintained. The relevant business and technical stakeholders must be involved in the IT DR planning process;
    i. ensure that IT DR planning is simple and practical and that systems that reduce the manual complexities of the recovery process are reviewed on a regular basis.
c. develop and maintain a structured training and awareness approach to ensure that all users of University IT resources and connected systems are aware and have a competent understanding of IT DR;
    i. ensure that all users of University IT resources and connected systems are made aware of and are responsible for having input into IT DR plans that affect their service areas;

ii. ensure that all aspects of the IT DR Policy are effectively communicated to the appropriate IT resources and University groups;
iii. ensure that all teams are educated in their respective IT DR roles and responsibilities;

d. integrate IT DR within risk and incident management processes including identifying, evaluating, and assessing potential disaster scenarios that could impact on critical activities;
e. integrate IT DR into the technical, operational, change, design and project management practices and procedures to promote a culture of resilience that will underpin the continuous delivery of services;
    i. ensure that processes are in place that identify any change(s) that would necessitate alterations to IT DR plans or environment. Changes affecting IT DR are not released without the necessary IT DR plan updates;
f. ensure that contracts related to the development or supply of IT systems provide assurances detailing system recovery times and potential data loss; and provide evidence of IT DR planning and regular testing;
g. ensure the continuous improvement of IT DR management and management practices;
    i. ensure that the IT DR Framework is 'fit for purpose' through testing, exercise, and internal and external audit programs;
    ii. schedule and conduct regular IT DR tests and exercises based on an agreed maintenance plan;
    iii. ensure that test outcomes reports are completed at the end of each exercise and detail the actions completed as well as remedial requirements for improvement;
    iv. ensure that the management and governance that supports the IT DR Framework are implemented effectively, maintained, and updated regularly.

Exemptions or Deviations

(10) Requests for exemption or deviations from IT DR technical or business requirements may be considered following the completion of an appropriate risk assessment. Requests for exemptions or deviations must be authorised by the Chief Information and Digital Officer, or the Chief Risk Officer and Deputy CIO and Director Information Technology. The Chief Information and Digital Officer will ensure that all exemptions are reviewed on a periodic basis.

(11) Prior to submitting a request, the following must be addressed:

a. define the control from which the exemption is being requested, and the reason for the exemption, as well as any introduced risk;
b. identify alternative controls that would mitigate the risk that might arise due to the exemption; and
c. obtain endorsement from the faculty or organisational unit requesting the exemption.

Section 3 - Procedures

(12) Nil.

Section 4 - Guidelines

(13) Nil.

Section 5 - Definitions

(14) The following definitions apply for the purpose of this Policy:

a. Controlled Entity (CE): means a person, group of persons or body over which the University has control. Refer to the Controlled Entities Policy for further details.
b. Maximum Allowable Outage (MAO) - the maximum amount of time the University can reasonably sustain an outage after the loss of an application or service. MAO is determined by the process owners.
c. Recovery Time Objective (RTO) - the time within which an application or a service must be restored during an IT DR event. The RTO specifies the time from when a recovery is initiated to its completion.
d. Recovery Point Objective (RPO) - the maximum tolerable extent of data loss for an IT application or service because of an IT DR event.
e. IT Disaster Recovery - the planning, running, and governing of activities to ensure that the University:
    i. identifies and mitigates operational risks that can lead to IT disruptions before they occur;
    ii. prepares for and responds to disruptive events (natural or otherwise, accidental, or intentional) in a controlled manner; and
    iii. recovers and restores IT systems that support critical University operations, within pre-defined timeframes and with known and acceptable data loss following a disruption.

Status and Details

Status	Current
Effective Date	12th April 2022
Review Date	12th April 2025
Approval Authority	Vice-President, Professional Services
Approval Date	12th April 2022
Expiry Date	Not Applicable
Responsible Executive	Eric Knight Deputy Vice-Chancellor (People and Operations)
Responsible Officer	Jonathan Covell Chief Information and Digital Officer
Enquiries Contact	Darrin Gay IT Disaster Recovery Project Manager