Cyber Security Policy

Section 1 - Purpose

(1) This Policy outlines how IT Resources are to be secured at the University and the responsibilities of staff and affiliates with access to the University's IT Resources.

Scope

(2) This Policy applies to users of Macquarie University IT resources and connected systems including:

a. staff employed by the University and its controlled entities;
b. affiliates including contractors, agents, honorary, clinical or adjunct appointees and consultants of the University.

Background

(3) Macquarie University (the University) is committed to maintaining a secure technology environment and as such, has established requirements to secure the University's IT Resources. Establishing these requirements aims to decrease the likelihood of negative consequences impacting the Confidentiality, Integrity and Availability of IT Resources.

Section 2 - Policy

Roles and Responsibilities

Role/Team	Responsibilities
Chief Information and Digital Officer (CIDO)	Ensuring this Policy and related artefacts align with the University's goals and applicable government regulations; Ensuring this Policy and related artefacts are reviewed and updated in accordance with operational needs; Sponsoring the implementation of cyber security controls to address identified risks; Approving (where warranted) exemptions to this Policy and related artefacts; and Overseeing cyber security incident response activities, as required.
Chief Information Security Officer (CISO)	Managing the day to day operations of the Cyber Security team; Reviewing and updating this Policy and related artefacts in accordance with operational needs; Ensuring the implementation of cyber security controls to address identified risks; Managing cyber security incident response activities, as required; and Reporting Information to the CIDO, as required.
Cyber Security team	Implementing cyber security controls to address identified risks; Providing cyber security guidance based on best practice, as required; Ensuring Third-Parties are aware of their cyber security responsibilities when receiving University Information or accessing University Information systems; Assisting in cyber security incident response activities, as required; and Reporting Information to the CISO, as required.

Role/Team	Responsibilities
Service Desk	Acting as a first point of contact for IT support requests; Providing basic troubleshooting and technical assistance for hardware and software issues; and Reporting cyber security events to the IT Cyber Security team.
Central IT	Implementation and maintenance of IT Resources to ensure reliability and availability of the University's services; Supporting with the implementation of security controls to address identified risks, as required; and Assisting in cyber security incident response activities, as required.
Managers and Supervisors	Ensuring staff under their supervision undertake cyber security awareness training; Ensuring staff under their supervision conform to this Policy and related artefacts; and Requesting the removal of access to University IT Resources and Information for staff when no longer required.
Staff who deploy or manage applications, computer or networking systems	Implementing IT Resources with security controls that align with the Computer and Network Security Policy; Maintaining the reliability and security of computer and networking systems; Decommissioning IT Resources and securely deleting Information; and Ensuring affiliates are aware of their cyber security responsibilities when receiving University Information or accessing University Information systems.
Third-Parties (contractors)	Meeting the requirements defined in contracts and Service Level Agreements (SLAs).
Vice-Chancellor	Ensuring staff and IT Resources comply with this Policy and supporting artefacts.
Audit and Risk Committee (ARC) and its subcommittee: Information Management and Technology Special Purpose Committee (IMTC)	Satisfying itself that management periodically assesses the adequacy of the University's Information security infrastructure (including cyber security).
All staff and affiliates	Complying with this Policy and related artefacts; and Reporting cyber security events to the IT Service Desk team or the IT Cyber Security team (cyber@mq.edu.au).

Acceptable Use of IT Resources

(4) IT Resources must be handled in accordance with the Acceptable Use of IT Resources Policy.

Information Handling

(5) Information should be generated, stored, processed and transmitted in accordance with the:

a. Information Classification and Handling Procedure;
b. Records and Information Management Policy; and
c. Privacy Policy.

Access Management

(6) Logical access to IT Resources should be managed in accordance with the Computer and Network Security Policy.

Network Security

(7) Network security controls should be implemented in accordance with the Computer and Network Security Policy.

Encryption

(8) The use of encryption should be conducted in accordance with the Computer and Network Security Policy.

Decommissioning & Destruction

(9) IT Resources should be decommissioned and destroyed in accordance with the Computer and Network Security Policy.

Software Development

(10) Software development activities will be conducted in accordance with the Secure Software Development Procedure.

Risk Management

(11) The University will assess, evaluate and manage cyber security risks in accordance with Confidentiality, Integrity and Availability requirements of IT Resources and Information:

a. this must be performed in accordance with the Risk Management Policy and Enterprise Risk Management Framework (ERMF); and
b. risks should be reviewed annually at minimum.

(12) A register documenting the University's cyber risks will be established. The register should include, at a minimum:

a. risk statement;
b. inherent risk rating;
c. current mitigating controls;
d. residual risk rating;
e. risk owner;
f. risk action; and
g. reference to a recommendations plan (if required).

(13) Third-Party risks should be managed in accordance with the Procurement Policy and the Risk Management Policy.

Human Resources

(14) All staff and affiliates with access to IT Resources should be screened in accordance with the Pre-Employment Checks Document.

(15) Contractual agreements between the University, staff and affiliates, should outline their respective cyber security obligations and responsibilities:

a. additionally, where appropriate, obligations and responsibilities contained within contractual agreements should continue for a defined period after termination (e.g., confidentiality requirements).

(16) Modifications and updates to this and all related policies must be communicated to all University staff and affiliates in a timely manner, using the University's official communication channels.

Incident Response

(17) An Incident Response Plan (IRP) should be defined and document the relevant roles and responsibilities and cyber

security incidents should be managed in accordance with the Incident Management Policy. The IRP should be reviewed and tested annually.

(18) University related cyber security events should be reported immediately to the IT Service Desk team or Cyber Security team (cyber@mq.edu.au), in accordance with the Acceptable Use of IT Resources Policy.

(19) University related cyber security incidents should be responded to in accordance with the IRP:

a. the University is not responsible for managing cyber security breaches to staff or student personal emails, accounts or devices.

Compliance and Exemptions

(20) Any exemption from this Policy should be sought from the Chief Information Security Officer (CISO).

(21) Breaches of this Policy will be managed in accordance with the applicable provisions of the Staff Code of Conduct and other relevant policy instruments.

Section 3 - Procedures

Software Acquisition

(22) The Cyber Security team should be involved in the process of acquiring Commercial Off-the-Shelf (COTS) software (e.g., Software as a Service).

(23) A risk assessment must be conducted prior to acquiring software solutions in accordance with the approved Cyber Data Protection Impact Assessment (DPIA) Checks Procedure.

(24) Software should be patched prior to deployment.

(25) Controls must be implemented commensurate with the application rating, in accordance with the Cyber DPIA Checks Procedure.

(26) Software nearing end-of-life should not be acquired unless there is a documented plan for mitigating risks associated with the lack of future updates and vendor support.

Backups

(27) Backups must be:

a. retained in accordance with the requirements specific to the IT Resource and its classification;
b. managed and maintained by the Operations Services team and Infrastructure and Cloud Operations team;
c. tested monthly; and
d. reviewed quarterly by the Operations Services team and Infrastructure and Cloud Operations team.

(28) Accurate and complete records of all backups must be kept.

(29) Backups should be retained for a period based on business importance as well as legislative and compliance requirements.

(30) Backup and recovery procedures should be documented and reviewed regularly.

(31) Backup strategies (e.g. full, differential and incremental) along with frequency, should comply with the security

and recovery needs of the University.

(32) Backup media should receive adequate physical and environmental protection.

(33) All backup Information should be afforded the same level of protection as the original Information based on its classification in accordance with the Information Classification and Handling Procedure.

Business Continuity and Disaster Recovery

(34) Resources involved in critical business processes should be identified and the timelines for restoration and recovery should be defined.

(35) A Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) should be defined and document the relevant roles and responsibilities. The BCP and DRP should be reviewed and tested annually.

(36) Business continuity and disaster recovery activities should be conducted in accordance with the:

a. Business Continuity Management Policy; and
b. Information Technology Disaster Recovery Policy.

Section 4 - Guidelines

(37) Nil.

Section 5 - Definitions

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

a. Confidentiality, Integrity, and Availability (CIA Triad) refers to the core principles of Information security, ensuring that Information is protected from unauthorised access (confidentiality), remains accurate (integrity), and is accessible when required (availability).
b. Information means any Information in either physical or electronic format that is generated, created, stored, purchased or received during the conduct of University operations.
c. Information Technology Resources, or IT Resources, includes, but is not limited to:
    i. All computers and all associated data networks and systems, internet access and network bandwidth, email, hardware, data storage, computer accounts, all OneID systems, media, software (both proprietary and those developed by the University) and telephony services.
    ii. Information Technology services provided jointly, or as part of a joint venture between the University and a research centre, school, institute affiliated with the University, a subsidiary organisation owned by the University or any other partner organisation.
    iii. Information Technology services provided by Third-Parties that have been engaged by the University.
d. Third-Party means an individual or organisation working under contract with the University.

Status and Details

Status	Current
Effective Date	23rd July 2026
Review Date	23rd July 2031
Approval Authority	Deputy Vice-Chancellor (People and Operations)
Approval Date	23rd July 2026
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	Andrew Karvinen Chief Information Security Officer