Third-Party Cyber Risk Management Policy

Section 1 - Purpose

(1) This Policy outlines the requirements to maintain the security of Macquarie University IT Resources which are operated and/or maintained by Third-Parties.

Scope

(2) This Policy applies to all Macquarie University (University) Staff who engage with Third-Parties and Third-Parties with access to the University's IT Resources.

Background

(3) The University is committed to maintaining a secure technology environment and as such has established requirements to manage Third-Party risks. By establishing these requirements, the University aims to reduce the risk attached to the use of Third-Parties.

(4) A Third-Party engagement is any written arrangement between the University or its controlled entities and a person, company or organisation which is external to the University, located in Australia or overseas.

Section 2 - Policy

(5) All Third-Parties engaging with the University are expected to protect the confidentiality, integrity, availability, non-repudiation and authentication of the University's Information and IT Resources, commensurate with the risks posed to them.

(6) Third-Parties with access to IT Resources should complete University cyber security awareness and training upon induction.

(7) All Information shared between the University and Third-Parties should be performed using an approved secure file transfer method.

(8) A risk assessment must be carried out for each Third-Party requiring access to IT Resources, and Information prior to entering into a contract or agreement, as per the 'Third-Party Risk Assessment' section of this Policy.

(9) Third-Parties must inform the University's IT Cyber Security team (cyber@mq.edu.au) of Relevant Cyber Security Incidents within 72 hours of detection.

(10) Third-Parties should agree to abide by the University's Cyber Security Policies.

Third-Party Acquisition

(11) Prior to entering into a contract or agreement, Third-Parties must be evaluated per the Procurement Policy, and the selection criteria outlined in the 'Third-Party Acquisition Criteria' Section of this Policy.

(12) Selection criteria of Third-Parties must be re-evaluated when expanding an existing relationship to include

different products or services.

(13) Cyber security clauses within contracts with Third-Parties providing services or technology related products to the University should be reviewed by the IT Cyber Security team, the Procurement team and the Office of General Counsel before execution.

(14) Decisions regarding the engagement of a Third-Party should be made in conjunction with the relevant business unit, the Cyber Security team, the Procurement team (where appropriate) and are subject to approval by the appropriate financial delegate, once the risks of engaging the Third-Party have been determined.

Third-Party Risk Management

(15) A register of the University's Third-Parties should be established, maintained and regularly reviewed by the Cyber Security team.

(16) A Third-Party cyber security questionnaire should be developed, maintained and regularly reviewed by the Cyber Security team.

Third-Party Risk Assessment

(17) Prior to entering a contract or agreement, the responsible area should engage the IT Cyber Security team to complete and submit an IT Security Third Party Checklist appropriate to the risk level it presents.

(18) Risk assessments should consider the information outlined in the 'Third-Party Risk Assessment Considerations' Section of this Policy.

(19) Third-Parties should be re-assessed periodically or when an existing agreement/contract expands to include additional/different products or services.

(20) Cyber-critical systems and associated third-party services must be formally reviewed at least every twenty-four (24) months, and additionally upon any significant changes or when an existing third-party agreement is modified to include new or altered products or services, to ensure ongoing security, compliance, and risk management.

Monitoring Third-Parties

(21) The division that engaged the supplier should monitor Third-Parties for non-conformance against the agreed security requirements.

(22) If a Third-Party has been identified as non-conforming, the engaging division should mitigate the risks associated with the identified non-conformance. The IT Cyber Security team will:

a. perform a risk assessment on the instance of non-conformance, as per the Risk Management Policy;
b. determine appropriate mitigation strategies to reduce the risk to the University; and
c. implement appropriate mitigation strategies in conjunction with the Third-Party.

Contract Termination

(23) When a Third-Party contract is terminated, IT division will action the following to maintain the security of its IT Resources:

a. deprovision access rights for relevant Third-Party personnel, in accordance with the Computer and Network Security Policy;
b. require that any University Information classified as Confidential or above be returned and Securely Deleted

from Third-Party infrastructure:

i. data deletion should be accompanied by an attestation of deletion from the Third-Party;

c. reassert information confidentiality requirements and intellectual property ownership determinations; and
d. ensure that all IT Resources provided to Third-Party personnel are returned.

(24) Third-Parties must provide the University with timely access to any data held on its behalf:

a. data must be delivered in a complete, accurate, and usable format, (e.g., CSV, JSON, XML) unless otherwise agreed; and
b. Third-Parties must not delay, withhold, or condition access to data and must ensure that retrieval is performed in a manner that supports the University's operational, legal, and regulatory obligations.

Compliance and Exemptions

(25) Any exemption to this Policy must be sought from the Chief Information Security Officer (CISO).

(26) Breaches of this Policy will be managed in accordance with the applicable provisions of the relevant policy instruments.

Section 3 - Procedures

Third-Party Acquisition Criteria

(27) The following selection criteria should be considered when evaluating a prospective Third-Party:

a. the Third-Party's reputation and history;
b. the University's prior history with the Third-Party;
c. the Third-Party's country of origin; and
d. the Third-Party's ability to deliver the required products or services.

Third-Party Risk Register

(28) The Third-Party Risk Register should include, at a minimum, the following:

a. the name of the Third-Party;
b. the services/products they offer;
c. key contacts;
d. the University Business Owner;
e. whether the Third-Party has access to University's IT Resources (and if they are critical);
f. whether the Third-Party has access to the University's Information (and the classification);
g. whether a cyber security questionnaire has been completed by the Third-Party; and
h. the risk level presented by engaging the Third-Parties for products and/or services.

Third-Party Risks

(29) To effectively manage risks posed by Third-Parties, the following should occur:

a. Third-Parties should be required to complete the cyber security questionnaire and provide the responses along with required supporting artefacts (e.g., evidence);
b. the IT Cyber Security team should review the responses to the cyber security questionnaire to determine the

level of risk the Third-Party will pose to the business; and

c. Third-Parties should be required to complete the cyber security questionnaire as part of their review cycle, for the University to determine if the level of risk posed by the Third-Party has changed.

Third-Party Risk Assessment Considerations

(30) Third-Party Risk Assessment considerations include:

a. recent assurance activities/independent audits conducted against the Third-Party (e.g., System and Organization Controls 2 - Type 2, Information Security Registered Assessors Program) and existing certifications (e.g., ISO 27001) maintained by the Third-Party;
b. the classification of the Information and/or IT Resources involved in the service;
c. the type, level and duration of access to be granted to the Third-Party (logical and/or physical);
d. the controls implemented and managed by the University to manage the Third-Party's access to the Information and/or IT Resources;
e. the controls required to be implemented or managed by the Third-Party;
f. if the controls of the service or product align with authorisation and authentication requirements defined within the Computer and Network Security Policy;
g. logging and monitoring capabilities (e.g., application logs);
h. data security capabilities (e.g., encryption);
i. continuity capabilities (e.g., backup services, disaster recovery services);
j. incident management capabilities;
k. physical security expectations; and
l. if the Third-Party uses its own suppliers (i.e., a Third-Party's Third-Party) to provide products or services to the University.

Third-Party Contract

(31) The person with delegated authority to approve a Third Party contract must ensure that the contractual terms and conditions with the Third-Party includes appropriate security arrangements so that the University is not exposed to an unacceptable level of risk. Where applicable, contracts or agreements should specify, at a minimum:

a. Information handling requirements (e.g., confidentiality, non-disclosure, data sovereignty):
    i. the University is to retain ownership of all University Information stored or processed by the Third-Parties; and
    ii. upon request by the University, Third-Parties should securely delete any Information they hold and provide proof of secure deletion;
b. the duration of the contract or agreement;
c. the level, purpose and duration of access to IT Resources and Information;
d. the requirement to adhere to the University's cyber security Policies;
e. any/all expectations regarding the Third-Party's security controls to ensure that they are aligned with the requirements of the University's cyber security Policies;
f. that the University reserves the right to conduct security audits of the Third-Party's conformance to the University's cyber security Policies, as deemed necessary;
g. any security requirements as mandated by the governing law and/or other legal or contractual obligations;
h. that individuals who have access to IT Resources or Information are bound by the contract with the Third-Party;
i. that a background verification is required for the Third-Party's personnel prior to them being provisioned access to the University's IT Resources and Information;

j. obligations to report and assist with the resolution of any security weaknesses and/or incidents or suspected incidents that may impact the products or services provided by the Third-Party;
k. the requirement to notify the University within 72 hours of detecting a Relevant Cyber Security Incident that occurs within the Third-Party's environment and has/may have an impact to the University:
    i. a notice that the University reserves the right to engage an independent auditor to review or observe any Third-Party incident response activities undertaken in the Third-Parties environment;
l. resilience and recovery requirements based on the criticality of the products or services provisioned by the Third-Party;
m. requirements for the return or disposal of IT Resources upon termination of the contract or agreement;
n. break clauses associated with failure to meet security requirements;
o. access to all logs generated by the Third-Party relating to the University's data and services;
p. use of any additional suppliers (i.e., fourth parties to the University) relied on by the Third-Party to deliver their products and/or services as part of the contract, and the obligations of the Third-Party to ensure their suppliers also meet the requirements of the contract; and
q. definition of key terms (e.g., incident, vulnerability, information) to avoid any misunderstanding.

Section 4 - Guidelines

(32) Nil.

Section 5 - Definitions

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

a. Information means any information in either physical or electronic format that is generated, created, stored, purchased or received during the conduct of University operations.
b. Intellectual Property means all forms of intellectual property rights throughout the world including copyright, patent, design, trademark, trade name, and all confidential Information including know-how and trade secrets.
c. IT Resource means any device or software that has value to the University and consequently needs to be suitably protected, including hardware (e.g., laptops, desktops, servers, network equipment, phones, printers, storage devices), and applications (e.g., cloud/desktop/server based).
d. Relevant Cyber Security Incident an actual event that originates from a cyber based threat, which impacts the confidentiality, integrity or availability of a product or service provided by a Third-Party.
e. Securely Deleted means the deletion of Information in such a way that it is unrecoverable (e.g., shredding, degaussing, cryptographic erasure).
f. Staff means an individual directly employed by the University.
g. 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