Vulnerability Disclosure Policy

Section 1 - Purpose

(1) This Policy outlines the University's Security Vulnerability disclosure program, which aims to provide a method for users to notify the University of any identified or suspected security vulnerabilities within the University's IT Resources or products.

Scope

(2) This Policy applies to any user with lawful access to Macquarie University's (the University's) IT Resources or products provided by the University. This includes:

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

Those listed above will be known as Users for the purpose of this Policy.

Background

(3) The University is committed to maintaining a secure technology environment and as such, believes in the responsible disclosure of potential security vulnerabilities. By establishing an official reporting channel, the University aims to remediate security vulnerabilities and therefore decrease the likelihood of malicious exploitation.

Section 2 - Policy

Reporting Protection

(4) To encourage responsible reporting, the University will not take legal action against a User who reports a Security Vulnerability, so long as the report is made in accordance with the requirements of this Policy.

Unauthorised Conduct

(5) Any User with access to the University's IT Resources must comply with Australian law, and not compromise or exploit the University's Information, personnel, infrastructure or operations. The following actions are not authorised, unless specifically approved by the University:

a. engaging in unlawful or unethical behaviour;
b. disclosing Security Vulnerability information publicly;
c. engaging in physical testing;
d. leveraging deceptive techniques (e.g., Social Engineering);
e. executing resource exhaustion attacks (g., Distributed Denial of Service);
f. leveraging automated vulnerability assessment tools;

g. introducing malicious software that could negatively impact the University;
h. reverse engineering the University's products or IT Resources;
i. modifying, destroying, or exfiltrating the University's Information;
j. hacking or penetration testing the University's IT Resources; and
k. accessing or attempting to access University accounts or Information.

Vulnerability Assessment & Mitigation

(6) Upon receiving a Security Vulnerability report, the University will:

a. analyse and evaluate the Security Vulnerability to determine its validity and potential impact to the University; and
b. take appropriate action to mitigate the Security Vulnerability.

Section 3 - Procedures

How to Report

(7) A potential Security Vulnerability can be reported to cyber@mq.edu.au and should contain the following information (where possible):

a. a detailed explanation of the potential Security Vulnerability;
b. the name of the product(s) and/or IT Resource(s) that may be affected;
c. the number of potential end Users affected;
d. detailed steps taken to identify and reproduce the potential Security Vulnerability;
e. evidence (g., proof-of-concept code/scripts, screenshots, screen recordings); and
f. the contact details of the reporter and whether they wish to be publicly acknowledged.

Outcome

(8) The University will:

a. respond to the User acknowledging receipt of the report within 2 weeks;
b. request additional information regarding the Security Vulnerability (if required); and
c. keep the User informed of the progress if requested.

(9) The University will not:

a. provide any financial compensation for the disclosure of a Security Vulnerability; or
b. share a User's details without permission.

Section 4 - Guidelines

(10) Nil.

Section 5 - Definitions

(11) 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. 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.
c. Security Vulnerability means a weakness in an IT Resource that can be exploited for malicious purposes.

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