Cyber Security Policy

Section 1 - Purpose

(1) This Policy specifies the cyber security responsibilities of Macquarie University staff, students, and other authorised users in order to protect the University's people, information, and technology assets.

Background

(2) Information and information systems are vital for delivering the University's broad range of functions and services. The University is committed to maintaining a respectful, safe, reliable, and secure technology environment that allows it to meet organisational objectives, contractual obligations, regulatory requirements, and ethical responsibilities.

Scope

(3) This Policy applies to:

a. all technology resources used by, operated by, or provided on behalf of the University (including its controlled entities);
b. all information collected, created, stored, or processed by, or for, the University on computer and network resources; and
c. all individuals who utilise, or are involved in deploying and supporting, computer and network resources provided by the University.

Section 2 - Policy

(4) It is the responsibility of all individuals who are provided access to information or information systems operated by, or on behalf of, the University to:

a. only access information, applications, and systems where access is authorised by the University;
b. access and make use of the University's computer and network resources in a secure and respectful manner;
c. maintain the security and confidentiality of information generated or collected by the University in accordance with the Information Classification and Handling Procedure;
d. handle information generated or collected by the University in accordance with the University's Privacy Policy and Records and Information Management Policy;
e. follow the cyber security guidance of the University delivered through training and awareness activities or communicated through official University channels;
f. refrain from deliberately damaging or reducing the security of University systems;
g. seek guidance from Macquarie Information Technology (IT) Cyber Security if unsure of secure practices; and
h. promptly report Suspicious Events, Data Breaches, or policy violations to their manager or supervisor and the IT Service Desk.

POSITION AND ROLE-SPECIFIC CYBER SECURITY RESPONSIBILITIES

(5) The Chief Information and Digital Officer (CIDO) is responsible for:

a. ensuring that this Policy and related procedures align with the University's goals and applicable government regulations, and are reviewed and updated in accordance with operational needs;
b. overseeing the treatment of critical security incidents that impact the University in accordance with the Vulnerability Management provisions in the Computer and Network Security Procedure;
c. sponsoring the implementation of agreed security controls to address identified risks; and
d. approving exemptions to this Policy or the Acceptable Use of IT Resources Policy and supporting procedures.

(6) The members of the University Executive Group are responsible for ensuring that within their portfolios:

a. all information collected, created, stored, or processed using the University's computer and network resources is handled and protected in accordance with this Policy and related procedures.

(7) Macquarie IT Cyber Security is responsible for:

a. authoring and requesting appropriate updates to this Policy and related procedures;
b. aligning this Policy and related procedures to comply with applicable government regulations; and
c. providing guidance to authorised users on best practice for cyber security.

(8) Managers and supervisors are responsible for:

a. ensuring individuals under their supervision undergo the cyber security training provided by the University, and are aware of this Policy, the Privacy Policy and related procedures before access is to University systems or information is granted;
b. promptly requesting the removal of access to University systems and information for individuals when no longer required; and
c. promptly reporting Suspicious Events, Data Breaches, or policy violations identified by or reported to them, to the IT Service Desk.

(9) University staff, students, and other authorised users who handle highly sensitive information, per the Information Classification and Handling Procedure, are responsible for:

a. only collecting or creating the information required for the designated purpose in accordance with the University's Privacy Policy;
b. only retaining the required information for the length of time necessary;
c. employing the additional security measures specified in the Information Classification and Handling Procedure for the computers and mobile devices used for handling highly sensitive information;
d. restricting access to information to only those who require access; and
e. promptly notifying the IT Service Desk in the case of a suspected Data Breach.

(10) University staff who deploy or manage applications, computer, or networking systems are responsible for:

a. implementing systems with security controls that align with the Computer and Network Security Procedure;
b. maintaining the reliability and security of computer and networking systems;
c. decommissioning systems and removing unneeded information in a secure manner;
d. ensuring third parties are aware of their cyber security responsibilities when receiving University information or accessing University information systems; and

e. promptly reporting Suspicious Events, Data Breaches, or policy violations to their manager/supervisor and the IT Service Desk.

Section 3 - Procedures

(11) Refer to the Computer and Network Security Procedure and Information Classification and Handling Procedure.

Section 4 - Guidelines

(12) Nil.

Section 5 - Definitions

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

a. Authorised means given explicit permission by the University to access University systems with the username provided;
b. Chief Information and Digital Officer means the person holding or acting in that position in the University, or any other person nominated by the Vice-Chancellor to exercise that role for the purpose of this Policy;
c. Data Breach means the accidental or deliberate access or exposure of University information to unauthorised parties;
d. Exemptions are defined as any deviation from the requirements of this Policy or the Acceptable Use of IT Resources Policy and related procedures;
e. IT Service Desk means the Macquarie IT function that provides direct IT support for staff, students, and other authorised users;
f. Macquarie IT means the Macquarie University Information Technology office;
g. Macquarie IT Cyber Security means the staff within Macquarie IT who are responsible for cyber security functions;
h. Suspicious Event refers to an unusual event or incident that raises concerns of fraud or system attack by malicious individuals; and
i. Technology assets means University computer and network systems that facilitate data access, processing, storage, or transfer.

Status and Details

Status	Current
Effective Date	29th April 2021
Review Date	29th April 2024
Approval Authority	Vice-President, People and Services
Approval Date	29th April 2021
Expiry Date	Not Applicable
Responsible Executive	Nicole Gower Vice-President, Professional Services
Responsible Officer	Jonathan Covell Chief Information and Digital Officer
Enquiries Contact	Andrew Wan Chief Information Security Officer Information Technology