Information Classification and Handling Procedure

Section 1 - Purpose

(1) This Procedure specifies the actions required to classify information that is owned or handled by Macquarie University and facilitate the application of appropriate security measures in accordance with the Cyber Security Policy.

Scope

(2) This Procedure applies to:

a. all information collected, created, stored, or processed by, or for, the University on computer and network resources; and
b. all individuals who handle information for the University.

Section 2 - Policy

(3) Refer to the Cyber Security Policy.

Section 3 - Procedures

Responsibilities and Required Actions

Information Handling

(4) Information must be handled in a responsible and appropriate manner. Before collecting, storing, or distributing information, University staff, students, and other authorised individuals must:

a. classify the information;
b. determine the length of time that the information needs to be retained and how the information can be securely erased when no longer required;
c. minimise the information (fields and records) that is distributed to only that which is required;
d. engage Macquarie IT to review the compliance of third parties who are required to receive the information; and
e. be protected while being transferred in accordance with the Encryption section of the Computer and Network Security Procedure.

(5) If confidential or highly sensitive information is shared with an unauthorised party, exposed in an uncontrolled location, or accidentally received, immediately notify your University manager / supervisor and the IT Service Desk.

Information Classification

(6) Information should be categorised into one of the following classifications. If the classification of information being handled is not clear, please raise a case with the IT Service Desk for clarification with Macquarie IT Cyber Security.

(7) The minimum security standards for protecting University information on computer systems and networks are established in the Computer and Network Security Procedure.

Classification	Description	Examples	Handling and protection
Public	Information is intended by the owner to be distributed to members of the public.	Marketing material Published research information Student course information Academic calendar Individual staff contact details	May be distributed without restriction.
Internal	Information that poses a moderate risk to the University if exposed in an unauthorised manner or damaged.	Teaching materials General intellectual property IT operational reports De-identified research data relating to individuals Individual student contact details Project documentation	May be distributed to Macquarie staff using systems and services endorsed for internal use by the CIDO. This is the default classification level for unclassified information.
Confidential	Information that poses a significant risk to the University if exposed in an unauthorised manner or damaged.	University premises access records Unpublished research data Strategy presentations and documents Financial records Audit reports Council papers Mailboxes containing student or staff correspondence De-identified research data relating to individuals	May be distributed to University staff who have a specific and appropriate need to receive the information. Information and fields must be limited to only that which is necessary. May only be processed or stored on systems and services endorsed for internal use by the CIDO.
Highly Sensitive	Information that poses a high regulatory, reputational or commercial risk to the University if damaged or exposed in an unauthorised manner. Personally identifiable information. Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. Personal health information. Information that a healthcare professional or medical research collects to identify an individual, determine appropriate care or perform research activities.	Bulk staff or bulk student contact information Identifiable digital activity and access records (including WiFi) Job applicant, staff employment or administration records Student academic or administration records Identifiable research data relating to individuals (including clinical) Patient or client medical records Passwords or private keys Cloud administration account credentials Examples of personally identifiable information are: full name, face, home address, email address (if private), ID number, passport number, vehicle registration plate numbers, driver's licence number, fingerprints or handwriting, credit card numbers, digital identity, date of birth, telephone number, login name, screen name or nickname. Examples of personal health information are: test or laboratory results, scan images, appointment details, prescriptions, billing details, medical history, mental and physical health conditions, health cover details, demographic details and genetic information. Credit card numbers – Payment Card Industry Data Security Standard requirements apply	Seek guidance from Macquarie IT Cyber Security before sharing data internally or externally. Additional security measures are required for the capturing, processing, and storing of highly sensitive information as indicated below.

Additional Requirements for Handling Highly Sensitive Information

(8) When capturing, processing, storing, or otherwise handling highly sensitive information University staff, students and other authorised individuals are required to request additional security controls on the computer systems and applications that they use. Additional controls may include:

a. multi-factor authentication for remote access to University systems and cloud applications;
b. multi-factor authentication for laptop and mobile device access;
c. encryption for cloud storage, computer disks and mobile devices; and
d. data backup facility that provides secure transport and storage.

(9) The above controls are provided by Central IT and may be different depending on the systems in use. To request the above controls please contact the IT Service Desk through OneHelp.

Section 4 - Guidelines

(10) Nil.

Section 5 - Definitions

(11) The following definitions apply for the purpose of this Procedure:

a. Information means the data captured in digital systems or physical artefacts that belongs to the University or is handled by or for the University.
b. Multi-factor authentication is the facilitation of authentication with two or more methods of authentication such username and password, smartphone soft token, hardware token, or USB key).

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