Information Classification Standard

Section 1 - Context

(1) This standard provides a consistent approach for the classification of RMIT Group data and information, referred to hereafter as 'Information', so that it can be properly and securely managed throughout its lifecycle.

(2) This standard also defines the minimum classification requirements to enable Information Custodians to meet their responsibilities and accountabilities and should be read in conjunction with the Information Classification and Handling Procedure.

Section 2 - Authority

(3) Authority for this document is established by the Information Governance Policy.

Section 3 - Scope

(4) This standard applies to all RMIT Group Information, in all formats, as defined in the Information Governance Policy, except data and information related to Australian national security and defence.

(5) This standard applies to all individuals who create, use, manage, handle or process RMIT Group Information, including RMIT Group staff, casual employees, contractors, visitors, honorary appointees and third parties.

(6) The RMIT Group is RMIT University and its controlled entities, referred to hereafter as RMIT.

Section 4 - Standard

Background

(7) According the Information Governance Policy, an individual assumes the role of an Information Custodian when RMIT Information is in their possession.

(8) Information Classification is administrative metadata that enables the secure and effective management of Information across its lifecycle and provides a mechanism for Information Custodians to meet specific responsibilities and accountabilities to protect Information in their custodianship.

(9) Information Classification includes Security Classification and Management Classifications.

(10) Information Custodians must follow the Information Classification and Handling Procedure on how to classify and handle Information.

Security Classification

(11) Security Classification (or security labelling) signifies the confidentiality requirements and enables the appropriate application of security protections and controls for Information. It functions similarly to a Protective Markings Scheme

under the Victorian Protective Data Security Framework (VPDSF).

(12) Security Classification is mandatory for all Information and must be applied by an Information Custodian at the point of Information creation or collection.

(13) Schedule 1 of the Information Governance Policy defines the different levels of Security Classification.

(14) The Security Classification of Information must be reclassified if its confidentiality changes, or if the Information is incorrectly classified across the Information lifecycle.

(15) Processes and systems must be designed to enable the effective implementation of Security Classifications including ensuring Information Custodians understand the controls and protections enabled by the Security Classification and its impacts to Information access, use and movement.

(16) Access, movement, and use of Information must be informed by the Security Classification.

Management Classifications

(17) Management Classifications are additional classifications which enable the management of Information across its lifecycle. They function similarly to the Information Management Markings (IMMs) under the Victorian Protective Data Security Framework (VPDSF).

(18) Management Classifications enable the identification of:

a. Institutional Data, Research Data and Unofficial Information as defined in Section 4 of Data and Information Lifecycle Management Procedure
b. Information subject to public records retention requirements outlined in the Retention and Disposal Standard
c. Information Domains within the Information Domain Register and accountable trustee(s) for Institutional Data
d. Information subject to the Privacy Policy
e. Information subject to legal privilege.

(19) Management Classifications enable an accurate and discoverable account of Information assets and may be applied by Information Custodians and administrative governance functions at any of the following levels:

a. individual record level
b. physical storage location level
c. information asset level
d. technology asset level
e. Information Asset Register level, implemented via the RMIT Information Domain Register.

Responsibilities

(20) Information Custodians are responsible for the proactive annual review of classification of Information under their custodianship.

(21) Information Stewards are responsible for providing an advisory role and support for operational data governance functions, in accordance with the Information Governance Policy and its resources.

(22) The Chief Data and Analytics Officer is responsible for delivery of the RMIT Information Domain Register as the enterprise Information Asset Register.

(23) The Chief Information Officer is responsible for delivery of Technology Assets, in accordance with the Information

Section 5 - Definitions

(Note: Commonly defined terms are in the RMIT Policy Glossary. Any defined terms below are specific to this policy).

Information Asset	A collection of Information, defined and practically managed so it can be understood, shared, protected and used to its full potential. Information assets support processes and are stored across a variety of media and formats (i.e. both paper-based as well as electronic material). Information assets have a recognisable and manageable value, risk, content and lifecycle.
Technology Asset	A store of Information Assets in digital format, represented as an IT Asset as specified in the Information Technology and Security Policy.
Information Asset Register	A central catalogue of Information Assets under RMIT custodianship, implemented via the RMIT Information Domain Register.

Status and Details

Status	Current
Effective Date	6th June 2024
Review Date	14th March 2028
Approval Authority	RMIT University Council
Approval Date	5th June 2024
Expiry Date	Not Applicable
Policy Owner	Fiona Notley Chief Operating Officer
Policy Author	Nicola Burgess Interim Executive Director, Technology
Enquiries Contact	Data Management and Governance

Glossary Terms and Definitions

"RMIT Group" - RMIT University and its controlled entities (RMIT Europe, RMIT Online, RMIT Vietnam, RMIT University Pathways)