Classification of Analytics Data Standard

Section 1 - Purpose

(1) This Standard enables rapid and agile decision making through access to data for analysis purposes while respecting privacy and confidentiality. It sets out the approach for classifying data held in data analytics environments, forming the foundation for controls to ensure availability of RMIT information in analytics environments is maximised for authorised users, only limiting where mandatory.

Section 2 - Authority

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

Section 3 - Scope

(3) This Standard applies to all members of the RMIT Group who have access to RMIT's information or information systems for the purposes of performing analytics, including staff, students, casual employees, contractors, visitors, third parties (suppliers), and agents of the organisation who are bound to RMIT policy where their contract of engagement with the University specifically provides for this.

(4) This Standard should be applied to all analytics environments viewed as strategic, not to platforms that are targeted for decommissioning within 2 years of the introduction of this Standard.

Section 4 - Standard

General

(5) Access to RMIT information and information systems can be logical or physical and is regardless of the information being held on RMIT's premises or at other locations.

(6) All individuals who use, author, or administer data for analytics are accountable for compliance to this Standard as identified in the relevant responsibility.

(7) The following requirements assist RMIT to:

a. identify the appropriate classification of data
b. ensure users are aware of their responsibility when using, producing, or sharing data.

Classification and Access Requirements

ID	Description	Responsibility
DAA-100	Data will have a classification as per RMIT's Security Classification Levels.	Data Author
DAA-110	Each object stored in an analytics environment will be identified with the highest level of restriction based on all data attributes held within the object.	Data Author
DAA-120	If data within an object is required to assist in analytics by users with a lower access authority, then the object should be replicated with the sensitive data transformed such that it is removed, tokenised, or otherwise obfuscated to render the data available under a lower classification.	Data Author
DAA-130	Processes should be implemented to identify or restrict the authoring of data that is not classified. Unclassified data should be treated as 'Protected' by default.	System Administrator
DAA-131	A regular review identifying unclassified data is to be performed, ensuring appropriate securing of the data and feedback to the responsible Data Author of need to classify all data.	Chief Data and Analytics Officer (CDAO)
DAA-135	Automated monitoring of data for inappropriate classification is to be undertaken where feasible.	System Administrator
DAA-137	Where automated monitoring of data for inappropriate classification is not feasible, an audit approach is to be taken, reviewing a sample of stored data.	CDAO
DAA-140	The data will be categorised into data domains, such that access can be provided at domain-specific classification levels. The data domains will align with RMIT's Conceptual Data Model. There may be various sub-domains to enable finer refinement of the audience for data. Any sub-domains will need to be agreed upon with the System Administrator to ensure roles can be defined with appropriate access.	Data Author
DAA-170	If access to data that is not appropriate to their access levels in the analytics environment is identified, then the user is to report the instance to the CDAO.	Users
DAA-180	Users are to identify and apply the appropriate classification of data they author.	Data Author
DAA-190	Users are to adhere to the intent of the security classifications when sharing data and information from analysis (e.g. don't share Restricted information to others that should not have access to that data).	Users
DAA-195	Data analytic reports or outcomes that contain restricted data must not be embedded/displayed in documents unless: 1. personal identifiable information is removed or de-identified, and 2. all the raw restricted data has be masked/washed, or 3. access to the report is appropriately restricted, and/or 4. the recipient is authorised to receive the report or outcome and adheres to the restrictions of sharing that data.	Users

Section 5 - Definitions

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

Conceptual Data Model (CDM)	The Conceptual Data Model provides a view of the categories of data that are captured and used across RMIT.
Data Author	A person bringing data to or producing data on the platform.
System Administrator	A person involved in the administration of the configuration of the environment and tools.
User	A person with access to the analytics platform.

Status and Details

Status	Current
Effective Date	21st July 2021
Review Date	21st July 2024
Approval Authority	Chief Data and Analytics Officer
Approval Date	22nd July 2021
Expiry Date	Not Applicable
Policy Owner	Nonna Milmeister Chief Data and Analytics Officer
Policy Author	Henrique Delamanha Mendonca Director, Data Management and Governance
Enquiries Contact	Data Management and Governance

Glossary Terms and Definitions

"RMIT Group" - The University, its controlled entities and strategic investment vehicles (known as the RMIT Group).