TITLE	STANDARD ON ENTERPRISE DATA CLASSIFICATION
Initial Approval Date	May 21, 2020
Date of next review	May 2025

Related Documents	• Policy on Enterprise Data Governance • Standard on Enterprise Data Governance • Records Retention Schedule • Regulation on the Conduct of Research • Policy on the Responsible Use of IT Resources • Cloud Data Directive • Act respecting access to documents held by public bodies and the protection of personal information • Act to establish legal framework for information technology • Archives Act

PART I – PURPOSE AND SCOPE

1.1 The purpose of the Standard on Enterprise Data Classification (Standard) is to:

- establish a framework for classifying Enterprise Data, in both, physical and electronic formats, based on their level of sensitivity, value and criticality to McGill University (University).
- mitigate risk by providing a reference for the determination of controls required to safeguard Enterprise Data.
- help in ensuring compliance with university policy and relevant legislation concerning access, protection and security of Enterprise Data.

1.2 This Standard is to be read in conjunction with the Policy on Enterprise Data Governance (Policy) and the Standard on Enterprise Data Governance.

1.3 Definitions, roles and responsibilities described in this Standard shall correspond to the definitions, roles and responsibilities established by the Policy on Enterprise Data Governance and its associated Standards.

1.4 The Standard applies to Enterprise Data, irrespective of its location or format.

1.5 The Standard applies to Members of the University Community, comprising of internal and external users.

PART II – DATA CLASSIFICATION TYPES AND GUIDELINES

2.1 Business and Technical Roles and Responsibilities

The classification of Enterprise Data is informed by an assessment of data sensitivity and value to the University. It is the responsibility of the Data Trustee, in consultation with Legal Services, and with the support of the Data Steward, Data Manager and those in Technical Roles, to assign the appropriate classification to Enterprise Data, based on the Guidelines for Enterprise Data Classification Levels provided below. In assigning classification levels, the Data Trustee shall consider the potential impact to the University in the event that the confidentiality, integrity, and/or availability of Enterprise Data are compromised.

2.2 Types of Enterprise Data

Enterprise Data includes three types of data: Regulated Enterprise Data, Protected Enterprise Data and Public Enterprise Data.

Regulated Enterprise Data: Information whose protection and use are mandated by law, regulation. Regulated Enterprise Data are confidential. The unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the University. The highest level of security controls should be applied to Regulated Enterprise Data.

Protected Enterprise Data: Information whose protection and use are governed by contract, or any McGill regulation, policy or directive because of its confidential nature (e.g., proprietary information, data critical to the University's operation, financial data). By default, all Enterprise Data that is not explicitly classified as Regulated or Public Data should be labeled as Protected Data. Depending on the case, the unauthorized disclosure, alteration or destruction of Protected Data could result in a significant to moderate level of risk to the University. Appropriate security controls should be applied to Protected Enterprise Data.

Public Enterprise Data: Information that is deemed accessible to the public and is not confidential. Some level of control is required to prevent unauthorized modification or destruction of Public Enterprise Data. If there is ambiguity with respect to the level of Data Classification, the Data is to be classified "Protected" until it can be reclassified.

2.3 Guidelines for Enterprise Data Classification Levels

There is no ideal quantitative system for determining the classification of a particular data element. In certain situations, the suitable classification may be more evident, such as when provincial or federal laws require the University to protect certain types of data. The following table serves as a guideline for classifying data.

Classification Level	Description	Examples
Level 1: PUBLIC	Applies to data that are readily available to the public.	• Press releases • Public access website pages • Published brochures • Published annual reports • Academic calendars • Campus maps • University-wide policies • Course descriptions • Employee business contact information
Level 2: PROTECTED	Applies to data that are intended for use within the University. Unauthorized external disclosure or inappropriate use, alteration or destruction of information would reasonably be expected to cause moderate to serious harm, (operational, reputational, financial) to the University, individuals, businesses, other third parties.	• Internal memos and communications • Minutes of unit meetings • Drafts of content • Planning documents • Documents containing proprietary information • Administrative procedures • Research grant application and agreement records • Research compliance protocols
Level 3: REGULATED	Applies to data that must be kept private under law or regulation. Pertains to information, including personal information that is sensitive both externally and internally. The inappropriate use, release, alteration or destruction of information would reasonably be expected to cause severe harm, (operational, reputational, financial) to the University, individuals, businesses, or other third parties.	• Personal information • Student records • Employee records • Legal files • Emergency security response plans • Passwords PINs and system credentials