POLICY NAME	POLICY ON ENTERPRISE DATA GOVERNANCE
Approving Body	Board of Governors
Initial Approval Date	May 21, 2020
Date of last review	N/A
Date of next review	May 2025
Executive Sponsor	Provost and Vice-Principal (Academic) Vice-Principal (Administration and Finance)

Related Documents	• Standard on Enterprise Data Governance • Standard on Enterprise Data Classification • 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, SCOPE, DEFINITIONS

1.1 Purpose

In order to manage McGill University's data as a strategic asset, sound principles of governance are required to ensure data quality, integrity, access, security, use, and disposal.

This Policy on Enterprise Data Governance establishes roles and responsibilities for managing McGill University data, as well as more detailed standards for the operational management of these data. It also assigns responsibility for overall data governance at McGill University to the Data Governance Steering Committee (DGSC).

1.2 Scope

All members of the McGill University Community are responsible for complying with applicable law and regulations and University policy with respect to Enterprise Data, as defined below.

Note about Research Data:

Research Data is defined as factual information and material, both physical and electronic, commonly accepted in the relevant scholarly community as necessary to validate research findings including, but not limited to, research proposals, laboratory records, progress reports, internal reports, and presentations. Research Data include all information or records of any sort related to the application for, performance of, or results obtained from the research in question.

The classification of Research Data is subject to the University's governance framework promulgated by University policies and regulations, and relevant provincial and federal regulatory frameworks, such as those described in the Tri-Agency Statement of Principles on Digital Data Management. This Policy and its associated Standards do not apply to Research Data.

1.3 Definitions

"Data": Recorded, ordered symbols (e.g., letters, numbers) that carry information. Data are the basic building blocks of information and knowledge. There are many types of data that can be categorized by form (digital, analog), purpose (thematic, spatial, temporal), processor (numeric, text), and media (documents, images, video, audio).

"Data Domain": A data domain usually specific to a certain University function that owns the system that supports that function. Data domains are specified in the Standard on Enterprise Data Governance and can be modified by the DGSC as required and include all data related to that function, whether it is used for direct operations, in government reporting, in strategic planning, or otherwise.

"Enterprise Data": Any data or records created or received by McGill University employees or other constituents in the performance or transaction of University business that are shared by Authorized Users across departments. Administrative data collected in the course of the University's research activities covered by McGill's Regulation on the Conduct of Research, as well as the regulations of the research sponsors. Enterprise Data include, but are not limited to, machine-readable data, data in electronic communication systems, data in print, and backup and archived data on all media.

"Information": Data that have been interpreted or translated to reveal the underlying meaning. For example, data can be processed and interpreted as words, statements, and ideas. Ultimately, information is generally specific to a particular domain (activity, process, function). Information may be presented in many formats (reports, images, tables, charts) and media (documents, sound recordings, photographs, video). Information is more valuable than data.

"Legitimate University Business Purposes": Lawful business purposes that are consistent with the context in which data are provided to the University, as well as considered as appropriate by reasonable University Community expectations.

"Internal Authorized User": A member of the McGill University Community (e.g. an employee, student, alumnus or alumna, appointee, etc.) who has been granted permission by the University, by virtue of the individual's role and responsibilities, to access certain data or systems that are part of McGill IT Resources.

"External Authorized User": A non-member of the McGill University Community who has been granted permission by the University, by virtue of the individual's role and responsibilities, to access certain data or systems that are part of McGill IT Resources.

PART II – INTRODUCTION, ROLES AND RESPONSIBILITIES

2.1 Introduction

Enterprise Data are a strategic asset of the University and its exclusive property. As such, they must be managed according to sound data governance practices and procedures. A description of the types of Enterprise Data to which this Policy applies is included in the Standard on Enterprise Data Governance. Enterprise Data may include institutional information subject to access and disclosure restrictions set forth in the McGill University Standard on Data Classification. Information identified by this Standard as Level 2 or Level 3 (Protected, Regulated) must be particularly protected.

Proper management of Enterprise Data facilitates access to data by those with academic or administrative responsibilities within the University. This Policy, the Standard on Data Classification, the Standard on Enterprise Data Governance, and other standards and procedures that may be established under the authority of the Data Governance Steering Committee inform members of the University Community of their responsibilities to classify, use, protect, and manage that data properly.

Enterprise Data are generally available on an as-needed basis to Authorized Users carrying out their University responsibilities, subject to other standards of data access and management that may be established to conform to the requirements of law or for the effective operation of the University and support of its mission. This Policy is intended to complement, not supersede, other relevant policies and laws that may be applicable to Enterprise Data, such as the Quebec Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information.

Members of the Senior Administration with responsibilities for policy development are responsible for applying laws governing data access and related issues.

2.2 Roles and Responsibilities

The University is the owner of Enterprise Data. Individual departments, units, or schools bear responsibilities for certain defined domains (types) of Enterprise Data. The Data Governance Steering Committee (DGSC), Data Trustees, Data Stewards, Data Managers, and those in Technical roles perform distinct functions and have particular responsibilities for Enterprise Data as described below and in more detail in the Standard on Enterprise Data Governance.

2.2.1 The Data Governance Steering Committee (DGSC)

The DGSC is a University committee that is part of the University's IT governance structure. The DGSC reports to the Provost and Vice-Principal (Academic) and the Vice-Principal (Administration & Finance) on the implementation and maintenance of the University's Policy on Enterprise Data Governance and its associated standards. DGSC members include representatives from Legal Services, Secretariat, Analysis, Planning and Budget, Information Technology Services, and other senior University management staff, as required by the DGSC. The DGSC may create subcommittees and other administrative working groups to carry out specific responsibilities. Specific responsibilities of the DGSC are defined in the Standard on Enterprise Data Governance.

2.2.2 Data Trustees

Data Trustees are identified for each domain or type of Enterprise Data and derive authority from their position within the University. Data Trustees are listed in the Standard on Enterprise Data Governance. Data Trustees act as advisors to the DGSC. Data Trustees are responsible for strategic planning, policy, and oversight of the domain of Enterprise Data in their functional areas. Data Trustees or their designees are accountable for establishing procedures and promulgating policies applicable to Enterprise Data applicable to their data domain. Among the roles defined by this Policy, the Data Trustee has the highest level of responsibility for the management of Enterprise Data and for the promotion of proper access, accuracy, privacy, integrity, security and availability of the data for which they have responsibility. Data Trustees are accountable for the activities of their designated Data Stewards, and Managers to whom they grant authority and access. Specific responsibilities of Data Trustees are defined in the Standard on Enterprise Data Governance.

2.2.3 Data Stewards

Data Stewards derive their authority by virtue of their position or by delegated authority from Data Trustees, and have strategic planning, standard setting, and oversight responsibilities for Enterprise Data in their functional areas. Data Stewards, or their designates, are responsible for evaluating requests for access to or the release of Enterprise Data and recommending policies, standards and procedures to promote proper access, accuracy, privacy, integrity, and availability of the data for which they have responsibility. Data Stewards are accountable for the activities of their designated Data Managers to whom they delegate authority. Specific responsibilities of Data Stewards are defined in the Standard on Enterprise Data Governance.

2.2.4 Data Managers

Data Managers are subject matter experts designated by Data Stewards and have administrative and/or operational responsibilities for the Enterprise Data in a particular subject area. Data Managers have day-to-day responsibilities for managing administrative processes and establishing business rules for effective data management.

The Data Manager may authorize or set constraints on specific uses of data within their data domain by data users outside the units. Data Managers are accountable for the security and quality of the data domains they manage, whether the data are collected or maintained directly by the Data Manager (or their staff), by data users in other University units or by external parties. Specific responsibilities of Data Managers are defined in the Standard on Enterprise Data Governance.

2.2.5 Authorized Users

Members of the McGill University Community are primarily consumers of Enterprise Data but have responsibilities with respect to bringing to the attention of their superiors' data issues that inhibit the use of such data for Legitimate University Business Purposes. Specific responsibilities are defined in the Standard on Enterprise Data Governance.

2.2.6 Information Systems Management

The CIO and Associate Vice-Principal Information Technology Services designates Technical roles for the management and security of data systems and the delegation of authority to individuals in such roles. Those in Technical roles establish goals, objectives and procedures to implement the policies and standards applicable to the University network and data systems containing or affecting Enterprise Data.

PART III – AUTHORITY TO APPROVE STANDARDS AND PROCEDURES

The DGSC established under this Policy has the authority to approve and repeal standards and procedures, which are secondary to and comply with this Policy.

PART IV – REVIEW

A review of this Policy and Standards shall be conducted by the DGSC every five (5) years, or whenever necessary to ensure legislative or statutory compliance, or when deemed necessary to do so in the best interests of the University.