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

Related Documents	• Policy 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, ROLES AND SCOPE

1. Purpose

This Standard to the Policy on Enterprise Data Governance outlines the roles, responsibilities, and scope of authority for the Data Governance Steering Committee (DGSC), Data Trustees, Data Stewards, and Data Managers. It defines "Enterprise Data," describes data types, and identifies the Data Trustees for each type.

2. Roles

The Policy for Enterprise Data Governance specifies roles within McGill's Enterprise Data ecosystem and the general roles and responsibilities of the Data Governance Steering Committee (DGSC).

3. Scope

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

PART II – DATA GOVERNANCE STEERING COMMITTEE

4. Role and Responsibilities of the Data Governance Steering Committee (DGSC)

a. Provide oversight for the effective management and protection of all Enterprise Data

b. Support efforts to develop and review policies, standards, or procedures related to Enterprise Data governance
c. Provide guidance on the application of the Policy on Enterprise Data and its associated Standards and resolve escalation of conflicts regarding the management of Enterprise Data that cross trusteeship boundaries
d. Communicate with the University community regarding Enterprise Data management and applicable policies, procedures, and standards
e. Recommend and oversee initiatives that enhance Enterprise Data management
f. Define functions and responsibilities of individuals with designated data management roles and maintain a list of individuals assigned to those roles within the University
g. Classify new or existing data elements that comprise Enterprise Data and identify applicable sources of authority for each type
h. Develop and oversee processes by which University constituents (faculties, schools, institutes, departments, units, individuals) consult with relevant Data Trustees or Data Stewards to ensure that the appropriate approvals have been obtained before Enterprise Data are disclosed to third parties.

5. Role and Responsibilities of Individuals in Data Governance Functions

Individuals in designated data governance roles may delegate their assigned responsibilities as appropriate. Fundamental responsibilities applicable to all roles include:

a. Observe ethical obligations applicable to Enterprise Data
b. Report violations of University policy or law to their superior in the data governance chain
c. Report instances of perceived risk to the security of Enterprise Data
d. Ensure the use of Enterprise Data is in the best interests of the University
e. Respect the confidentiality and privacy rights of individuals
f. Access and use Enterprise Data for legitimate University purposes only
g. Complete training applicable to the role and seek any additional information needed to understand and perform the role and fulfill its responsibilities

6. Role and Responsibilities of the Data Trustee

Relative to other roles, Data Trustees have the ultimate responsibility for managing Enterprise Data in compliance with applicable University policies and legal and regulatory requirements. Data Trustees shall be knowledgeable of applicable laws and regulations relevant to the Enterprise Data over which they have responsibility. Additional responsibilities of Data Trustees include:

a. Promulgate policies within scope of responsibility relevant to Enterprise Data
b. Oversee the implementation of applicable laws and regulations and University policies, standards, procedures and guidelines with respect to data access and management
c. Determine and maintain records of the appropriate classification level for data domains in accordance with the Standard on Enterprise Data Classification .

d. Assist the DGSC in determining trusteeship of shared data elements that cross multiple units or divisions and in efforts to minimize multiple repositories for the same data. For example, name, ID, and other personal information are collected and/or used in multiple systems, such as financial, human resources, and student systems
e. Evaluate and determine high-risk and atypical requests for access to Enterprise Data within scope of responsibility.
f. Review and make a determination on requests for new uses of Enterprise Data or collections of data within scope of responsibility (e.g., transfer of Enterprise Data to internal or third-party repositories, databases, or applications).
g. Determine criteria and differentiate requests requiring business approval from requests related to technical roles .
h. Select appropriate Data Stewards, document these appointments, and communicate these selections to the Data Governance Steering Committee (DGSC)
i. Communicate the scope of responsibility and authority to those designated.

Ultimate responsibility for the relevant Enterprise Data domain rests with the Data Trustee regardless of delegation of authority to other positions.

7. Role and Responsibilities of the Data Steward

a. Ensure that applicable data quality and data definition standards are met
b. In cooperation with Data Managers and various Technical roles, establish authorization procedures to facilitate appropriate data access and ensure security for that data.
c. Define standards for documentation of data elements.
d. Develop standard definitions for data elements within scope of authority, including those that cross multiple units or divisions. For example, establish a uniform definition of "full-time employee" or unique definitions as appropriate for each data element.
e. Ensure that documentation exists for each data element, including at a minimum: data source, data provenance, data element business name, and data element definition.
f. Oversee data accuracy and integrity and implement programs for data quality improvement.
g. Perform appropriate review of user access for information systems that work with confidential information identified under the Standard on Enterprise Data Classification .
h. Decide on requests for access to Enterprise Data within the Data Steward's functional area, specifying the appropriate access procedure, and ensuring appropriate access rights and permissions according to data classification. Communicate the restrictions of the data classification. Consult Data Trustee for atypical or high-risk requests for access. Ensure that any appropriate agreement is in place prior to granting access to Enterprise Data.
i. Select and oversee Data Managers and ensure their assigned responsibilities are adequately and consistently fulfilled.
j. Support efforts to educate users about responsibilities and best practices in the management of data. .
k. Consult Data Managers and McGill University Community Users, as appropriate, to promote effective Enterprise Data management and protection.

l. Coordinate with Technical Data management roles with respect to data retention, disposition, preservation.
m. Recommend appropriate policies related to the management of Enterprise Data.
n. Evaluate risk for specific uses of data.
o. Ensure appropriate generation, use, retention, and disposal, of data and information consistent with University policies.
p. Ensure separation-of-duties structures are present, effective, and verified, where required.
q. Resolve issues in data element definitions across data types.
r. Work with the University's Procurement Services to ensure that obligations for data management are incorporated as in agreements with third parties to which the University grants access or rights to Enterprise Data. Consult with Legal Services and/or University Procurement Services, as needed.

8. Role and Responsibilities of the Data Manager

a. Decide on requests for the use or access to Enterprise Data for Legitimate University Business Purposes (as opposed to technical support/management purposes).
b. Apply the principle of "least privilege" (granting only the access needed to perform the required tasks) and work with technical staff to understand and implement security controls governing systems under the Data Manager's control.
c. Comply with applicable laws and University policies, standards, procedures and guidelines with respect to data access and management.
d. Instruct University users in proper handling of Enterprise Data within Data Manager's scope of authority.
e. Document data definitions for each data element (e.g. source, provenance, business name, definition) within the domain of Data Manager's operational unit(s). Communicate data definitions and/or recommended changes to existing definitions to the Data Steward. Resolve conflicts in data attributes.
f. Identify overlapping domains of authority with Data Manager's area of responsibility and coordinate or escalate to Data Steward when clarification is needed, or operational changes should be considered.
g. Create processes and procedures to ensure the accuracy, privacy and integrity of the Enterprise Data for which they are accountable.
h. Identify data warehouse reporting needs in particular data elements and attributes required to support inquiry and reporting needs.
i. Review and monitor compliance with data management standards, procedures and processes.
j. Recommend policies or modifications of polices to Data Stewards and Data Trustees
k. Communicate material changes to applicable policies and procedures to authorized users, and other University constituents.
l. Determine business rules for data updates when multiple data sources exist, in cooperation with Technical Data roles.
m. Report security and privacy risks to the DGSC through the Data Trustee.

9. Role and Responsibilities of Internal Authorized Users

a. Use University data for Legitimate University Business Purposes.
b. Bring to the attention of the Data Manager or Data Steward issues or inconsistencies with the data that inhibit the answering of business questions that support the functioning of the University.
c. Comply with all University data governance standards.

10. Role and Responsibilities of External Authorized Users

a. Use University data for Legitimate University Business Purposes solely as outlined in required contractual or confidentiality agreements entered into with the University.

11. Technical Roles and Responsibilities

11.1 Chief Information Officer and Associate Vice-Principal (Information Technology Services)

IT leader who manages defined IT functions and serves in a governance role with respect to Enterprise Data. The following IT guardian responsibilities are to be performed in collaboration with Enterprise Data management business roles, and in accordance with applicable laws, regulations and University policies, standards, procedures and guidelines with respect to data access and management:

a. Establish a secure environment for Enterprise Data.
b. Ensure operational continuity by providing solutions to back up Enterprise Data according to schedules determined in collaboration with Enterprise Data roles and establishing data restoration protocols.
c. Assign technical tasks and responsibilities and provide systems and technical support to facilitate data management activities.
d. Ensure the appropriate management of technical projects relevant to Enterprise Data management.
e. Advise and assist Data Trustee/Steward in assessing and mitigating risks to Enterprise Data management.
f. Assist Data Trustees/Stewards in resolving conflicts relating to access to Enterprise Data.
g. Ensure appropriate controls are in place to assure data confidentiality, integrity and availability.

11.2 Technical Data Steward

a. Technical Data Stewards work with the Data Steward on the same Data Segment. They have operational responsibility for the maintenance of the data repositories and system environments that support the application or applications associated with the Data Segment.

b. Establish technical procedures and processes for granting, revoking, and monitoring of access to Enterprise Data.
c. Establish processes and procedures for the retention, disposition, and preservation of Enterprise Data at the direction of Enterprise Data Trustees/Stewards and in compliance with University policy.
d. Establish and maintain approved and prioritized data feed requests based on rules provided by Enterprise Data Trustees, Stewards, and Managers.
e. Authorize and periodically review administrator and other privileged or elevated access requests for users in technical roles.
f. Depending on the organizational structure of the unit, they may be a member of the Data Steward's staff, or they may be assigned by the CIO from IT resources.
g. Evaluate security of delivery modes for transmission of data depending on the classification of the data
h. Deliver data or data-feeds as authorized.

12. Enterprise Data Subsets and Trustee Positions

The table below outlines the main data domains of McGill University's Enterprise Data and the Data Trustees for each. Enterprise data not covered by any the types below are nevertheless subject to applicable laws, policies, and regulations. Data that fall into multiple categories may have more than one responsible Trustee. Classification conflicts are resolved according to the roles and responsibilities outlined above.

Data Category	Data Domain Type	Trustee	Description/Notes
People – Personal	Donor /Alumni	Vice-Principal University Advancement	
	Employee /Retiree	Associate Vice-Principal Human Resources	Employee file, collective agreements, pension
	Student	Registrar	
	Student Health	Executive Director Services for Student	Student medical records
Space	Space	Associate Vice-Principal FMAS	Facilities, Campus, Physical assets and security
Organization	Financial	Associate Vice-Principal Finance	Financial forecasts and reporting
	Procurement	Associate Vice-Principal Finance	Vendors, Contracts, Tenders
	Sales	Associate Vice-Principal FMAS	Auxiliary services: Parking, Bookstore
	Academic programs	Provost	Curriculum
	Governance and Regulatory	Secretary-General	Records and corporate documents, access requests, institutional policies; University

			records related to academic tenure and promotion processes, academic grievances, student grievances and appeals
	Risk Management	Vice Principal Administration & Finance	Risk assessments, Audits
	Information Technology	CIO	Infrastructure and IT security (access identity) , IT assets
	Legal	General Counsel and Director of Legal Services	Legal opinions, legal cases before the court
	Library	Trenholme Dean of Libraries	Collections, catalogs
	Institutional Planning & Performance	Exec Director APB	Measures, Analytical data sets, Budget
	Public Web/Social-Media Content	Vice-Principal (Communications and External Relations)	Branding, web analytics Internal communications, External relations (e.g. Government and regulatory bodies, external communications)
	Research Management	Vice-Principal (Research & Innovation)	Administration (e.g. grants, applications, agreements, intellectual property)

13. Definitions

13.1 Access: The right to read, enter, copy, query, download, or update data.

13.2 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).

13.3 Data Domain: A data domain usually specific to a certain University function that owns the data that supports that function. Data domains are specified in the Standard for 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.

13.4 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.

13.5 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.

13.6 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.

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

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