Policies, Procedures and Guidelines

Complete Policy Title	Policy Number (if applicable)
Data and Information Classification Policy	
Approved by	Date of Most Recent Approval
President and Vice-Presidents	**April 12, 2022**
Date of Original Approval(s)	Supersedes/Amends Policy dated
	IS-08 2016
Responsible Executive	Policy Specific Enquiries
Provost & Vice-President Academic **Vice-President Operations & Finance**	
	General Policy Enquiries
	Policy (University Secretariat)

DISCLAIMER: *If there is a Discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails.*

TABLE OF CONTENTS

SECTION I: INTRODUCTION....................1

PREAMBLE AND SCOPE....................1

SECTION II: TERMS AND DEFINITIONS....................2

SECTION III: DATA AND INFORMATION CLASSIFICATION....................5

RESTRICTED DATA AND INFORMATION....................5

CONFIDENTIAL DATA AND INFORMATION....................5

INTERNAL DATA AND INFORMATION....................6

PUBLIC (UNRESTRICTED) DATA AND INFORMATION....................6

APPENDIX A: RELATED POLICIES AND LEGISLATION....................7

SECTION I: INTRODUCTION

PREAMBLE AND SCOPE

1. This Policy provides the basis for protecting the confidentiality of data and information in the custody or control of the University, based upon its level of sensitivity, value and criticality to the University. The classification of data and information will aid in determining baseline security controls for the protection of data and will assist in the protection of data and information.

2. Data and information are enterprise assets in the custody or control of the University and are accessible and used for institutional purposes by authorized users and are protected according to classification under this Policy. Some data assets are owned by the University, while other data assets and information are collected and held by McMaster as a custodian, not an owner. These critical assets are used for institutional planning and operations and must be protected to reduce risk and support compliance with legislative requirements.

3. This Policy applies to all Members of the University Community ("**Community Members**") including, but not limited to, students (graduate, undergraduate, and continuing education), staff, faculty, medical residents, volunteers, visitors (including visiting professors), contractors, and institutional administrators and officials representing McMaster University.

4. This Policy applies to all data and information created, collected, stored, or processed in all University Faculties, departments and units and is applicable to all university employees, contractors and students who create and use University data and information. The exception to this is data that is generated from research.

SECTION II: TERMS AND DEFINITIONS

5. For the purpose of interpreting this document:

   a) Words in the singular may include the plural and words in the plural may include the singular;

   b) **Authorized User** means a Community Member who has authorization to access data and information that is in the custody or control of the University;

   c) **Community Member** includes, but is not limited to, students (graduate, undergraduate, and continuing education), staff, faculty, medical residents, volunteers, visitors (including visiting professors), contractors, and institutional administrators and officials representing McMaster University.

   d) **Confidentiality** refers to the obligation of an individual or organization to safeguard entrusted information. The practice of confidentiality includes obligations to protect information from unauthorized access, use, disclosure, modification, loss or theft;

   e) **Data** means items of information that are collected, maintained, and utilized by the University for the purpose of carrying out institutional business. Data is typically comprised of numbers, words or images. The format and presentation of data may vary with the context in which it is used. Data are the basic building blocks of information and knowledge.

   f) **Data Stewards** are University employees who hold formal decision rights and accountabilities for the University's data in their Domain. They are responsible for verifying the quality and integrity of data and data-related assets in their domain and will support those processes using established data management procedures to effectively manage the data. They authorize the use of data within their domain and monitor this to verify appropriate data access.

   g) **Employee** refers to staff (see below) and faculty (see below);

   h) **Faculty** are defined as academic teaching staff, clinical faculty, and senior academic librarians who are members of the "teaching staff". Teaching staff as defined in the *McMaster University Act* means the employees of the University or of a college affiliated with the University who hold the academic rank of professor, associate professor, assistant professor or lecturer.

   i) **FIPPA** means the *Freedom of Information and Protection of Privacy Act.*

   j) **Information** means **data** that have been derived, interpreted, processed, translated, structured or translated and presented to reveal the underlying meaning. For example, data can be processed and interpreted as words, statements, and ideas. Information may be presented in many formats (report, dashboard, graphic visualization, Key Performance Indicators (KPIs) or as a corollary database, Data Mart or Data Warehouse. Information is more valuable than data;

   k) **Limited Internal Use** means authorized McMaster users may use the data or information only for McMaster University internal business purposes.

l) **PCI – DSS** means Payment Card Industry – Data Security Standards requires any organization that collects, processes, transmits or stores cardholder data, to uphold and maintain the data security standards that are set by the payment industry worldwide, and which are managed by the PCI Security Standards Council (PCI SSC);

m) **Personal Data** means Data that contains personal information about an identifiable individual as defined in the *Freedom of Information and Protection of Privacy Act* (FIPPA). This data, if compromised or used inappropriately, would have implications to the privacy of an individual;

n) **Personal Health Information (PHI)** means data that contains personal health information about an identifiable individual. This data, if compromised or used inappropriately, would have implications to the privacy of an individual. Such incidents must be reported to the university privacy office. If compromised or used inappropriate, harm may be caused to the individual;

o) **PHIPA** means the *Personal Health Information Protection Act*. PHIPA governs the manner in which personal health information may be collected, used and disclosed within the health sector;

p) **Personally Identifiable Information (PII)** means information that can be used to uniquely identify, contact, or locate an individual or can be used with other sources to uniquely identify a single individual. If compromised or used inappropriate, harm may be caused to the individual;

q) **Research Data** means Data that is collected by or derived from research, scholarly, and artistic activities;

r) **Semi-Structured Data** means Semi-structured data is unstructured data with some structured metadata (internal tags and markings that identify separate data elements), which enables information grouping and hierarchies. Examples would be data on the web such as XML, JSON, YAML and other markup languages, email data, and electronic data interchange (EDI);

s) **Staff:** Employees of the University including, but not limited to: The Management Group (TMG), unionized employees, temporary employees, casual employees, non-teaching staff[1], Sessional Faculty, Post-doctoral Fellows, and Teaching Assistants;

t) **Structured Data** means Structured data fields are aligned side by side in fixed or variable record lengths with specific data fields appearing at specific locations within each record. Structured data is represented by a data model that is defined by a schema in a database. It can be queried using Structured Query Language (SQL) since the structure of the data is known;

[1] "non-teaching staff" means the employees of the University and of a college affiliated with the University who are not members of the teaching staff –The McMaster University Act, 1976

u) **Third Party Data** means data that is created or owned by a third party and is being used in support of academic, research or administrative activities. This data if compromised or used inappropriately would have implications for the third party. This includes data such as licensed software or software components, and copyrighted material; and

v) **Unstructured Data** means data that is not associated with a given fixed structure (schema or model or organized in any way). This includes non-textual data such as images, multimedia files, sound files, or a record consisting of text such as a word-processed file, email, blogs, wiki posts, or social media posts.

SECTION III: DATA AND INFORMATION CLASSIFICATION

6. All Data and Information at the University shall be assigned one of the following classifications. Note that collections of diverse data sets shall be assigned the most secure classification of an individual data or information component in the aggregated information.

RESTRICTED DATA AND INFORMATION

Description	Data and Information of a highly sensitive or confidential nature which is: a) intended for restricted internal use; b) stored securely at the University; c) restricted to approved University use; and d) protected by University policy, federal or provincial legislation, or standards.
Risk	Disclosure, loss or unauthorized access or modification of this information may cause *significant risk* to the University and would have serious adverse effects on an individual, a group or, University operations, assets, or reputation and has a significant potential of liability.
Examples	○ confidential financial information, including credit card and banking information ○ passwords and access codes ○ personal health information (PHI), including Health Card Numbers ○ Personally Identifiable Information (PII), including Social Insurance Numbers, employee numbers, and student numbers ○ Strategic financial and personal data, and strategic organizational plans

CONFIDENTIAL DATA AND INFORMATION

Description	Data and information of a sensitive or confidential nature which is: a) intended for limited internal use; and b) limited to access by individuals in specific University functions.
Risk	Disclosure, loss or unauthorized modification of confidential information would cause a *moderate risk* to the University and have moderate adverse effects on an individual, a group or, University operations, assets, or reputation and has a high potential of financial or legal consequences.
Examples	○ confidential facilities plans (gas, water, hazardous materials) ○ equity and diversity information ○ third-party information (vendor agreements, Request for Proposal (RFP) submissions, Purchase Orders (PO), etc.)

INTERNAL DATA AND INFORMATION

Description	Data and Information that is available to Community Members who have a clear need for access as part of their employment or affiliation with the University.
Risk	Disclosure, loss or unauthorized modification of internal information would have *minimal risk* to the University and, if not available, could disrupt the business but would have minimal impact on an individual, a group, safety, assets or liability.
Examples	○ basic floor plans ○ contracts or requisitions that do not have a confidentiality clause ○ internal policies and procedures ○ non-personally identifiable student or employee information ○ routine business communications and documentation

PUBLIC (UNRESTRICTED) DATA AND INFORMATION

Description	Data and Information that is generally available to all employees, students, and in the public interest.
Risk	Disclosure, loss or unauthorized modification of unrestricted information has no effect on an individual, group, or University operations, assets or reputation.
Examples	○ aggregated and de-identified institutional information approved for publication ○ campus maps ○ employee directory ○ employment postings ○ published information, including program brochures and class schedules

APPENDIX A: RELATED POLICIES AND LEGISLATION

This Policy is to be read in conjunction with the following policies, statements, and legislation. Any question of the application of this Policy or related policies shall be determined by the Vice President (Operations and Finance) in conjunction with the administrator of the other policy or policies. The University reserves the right to amend or add to the University's policies and statements from time to time (this is not a comprehensive list):

- Closed Circuit Television Surveillance Policy
- Freedom of Information and Protection of Privacy Act (FIPPA)
- Journal Entry Policy
- Payment Card Industry – Data Security Standards
- Personal Health Information Protection Act (PHIPA)

Privacy Governance and Accountability Framework

- Access to Personal Health Information, Policy on
- Background Check Policy
- E-mail Protocol for Personal Information and Personal Health Information
- Handling of Personal Health Information (PHI), Policy for the
- Handling of Personal Information, Policy for the
- Obtaining Consent re Personal Health Information (PHI) to be Transmitted via Email, Guideline on
- Portable Storage and Mobile Devices Policy
- Privacy Breach Protocol

University Technology Services (UTS) – Policies and Procedures

- Information Security Policy
- Information Storage Guidelines
- Mac ID Terms and Conditions of Use