BRAMPTON

COUNCIL POLICY

Category: Governance

Information and Data Governance Policy

Policy Number: [Policy Number (assigned by CAO's Office, after approval)]
Approved by: Choose an item. [Council Resolution #] – [Date]
Administered by: [Division and section]
Effective Date: [Date]

Contents

1. Background

At the City of Brampton ("the City"), Information Assets (records, information and data) are created, received, and used every day. These assets facilitate day-to-day business activities and allow the City to make sound business decisions when determining how, when and what types of services it provides.

Information and Data Governance (IDG) identifies risks, maintains quality controls, and brings consistency to the way that the City manages its assets. It ensures that as an organisation, we obtain maximum value from our information, and allows for these assets to be leveraged, while complying with legislation.

To sustain the continuing conduct of business, and ensure accountability, the City will integrate information and data governance into all its business processes. The IDG program is sponsored jointly by the City Clerk's Office and the Information Technology Division, with the support of the Corporate Leadership Team

2. Purpose

The purpose of this Information and Data Governance Policy is to provide clear direction on the establishment, development and maturing of the policies, processes and procedures that inform how the City creates and manages its enterprise-wide information assets.

The City aims to be a leader in enterprise information and data governance where value from information assets is leveraged, and the growing challenges of privacy, security and governance are met by:

- Developing best practices for effective data management and protection.
- Ensuring the City's Information Assets are available and can be leveraged as and when appropriate.
- Ensuring that a data trail is effectively documented within the processes associated with creation, accessing, retrieving, exchanging, reporting, managing, storing, and deletion of data.
- Protecting the City's data against internal and external threats (e.g. Privacy Breach, or Security Breach).
- Establishing clear lines of accountability.
- Defining the lifecycle for the capture, creation, usage, sharing, and disposition of the City's Information Assets.

Ensuring that the City complies with applicable laws, regulations, exchange and standards.

3. Application and Scope

This Council Policy applies to all corporate information assets including records, information, and data. The Policy will support the process of managing the

availability, usability, integrity, and security of information and data stored in City systems, based on internal standards, policies, controls, and governance best practices.

3.1 Exceptions

This Council Policy does not apply to political information assets of Councillors.

4. Outcomes

4.1 **Application Licensing Management** – Ensures the City complies with its software licensing agreements for on-premises and cloud-based solutions.

4.2 **Business Continuity** – Reduce risks by ensuring technology is incorporated into the City's continuity and disaster recovery plans.

4.3 **Business Intelligence** – Ensures the City's information assets are used to extract insights to make faster, more informed decisions.

4.4 **Defensible Disposition** – Identifies proved strategies to control information by actively sorting out what data needs to be retained, from data that can be securely dispositioned.

4.5 **E-Discovery** – Ensures information assets have an approved method of identifying, collecting, and producing electronically stored information to be presented in court, or to respond to an Access to Information Request.

4.6 **Enterprise Application Selection & Implementation** - Enhances internal processes and business activities as well as ensures application-related risks are identified and managed up front for business-critical and non-business critical applications.

4.7 **Legacy Systems Management** – Enables analysis of the City's legacy systems, which is critical to day-to-day operations, ensuring their migration and replacement is carefully assessed and planned to minimize potential risks.

4.8 **Legal Holds** – Enables the City to preserve all forms of potentially relevant information when litigation is pending or reasonably anticipated.

4.9 **Legislative Compliance** – Enables the City to comply with various Federal, Provincial, Regional and Municipal legislation, regulations, and industry standards.

4.10 **Lifecycle Management** – Recognizes that information assets have different value and require different approaches as it moves throughout its lifecycle, specifically: creation or collection, processing, dissemination, use, storage, and disposition.

4.11 **Managed Access** - Protects the confidentiality and integrity of vital information assets.

4.12 **Managed Assets** - Ensures that records, data, information, knowledge and content are all treated as assets - avoiding increased risk and cost due to data and content misuse, poor handling, or exposure to regulatory scrutiny.

4.13 **Managed Incidents** – Ensuring the City can quickly identify and mitigate potential threats before they cause serious damage.

4.14 **Managed Infrastructure** - Maximize employee productivity by improving the performance of technology systems, increasing uptime, and enhancing the user experience.

4.15 **Managed Master Data** – Ensures the quality of the City's data by ensuring that identifiers and other key data elements about those entities are accurate and consistent, enterprise-wide.

4.16 **Open Data/ Open Government** – Ensures transparency and allows for residents and businesses to use the City's data to analyze markets, predict trends and requirements, and direct businesses in their strategic investment decisions.

4.17 **Policy Compliance** – Ensures compliance with City policies, by-laws, standard operating procedures (SOP), guidelines and best practices when decision-making.

4.18 **Real-time Insights** – Ensures the City is able to visualize and understand changing business requirements and client-driven demands in order to make timely, data-driven decisions.

5. Principles

5.1 **Availability** – Information should be readily available when and where it is required in a timely, efficient and accurate manner. Business processes and activities are to be documented in an open and verifiable manner and be made available to all staff and public as required.

5.2 **Integrity** – Information assets that are being managed by the City must be authentic and reliable. The City must ensure the accuracy and validity/consistency of City information and data resources/ assets. Data standards must be defined and managed throughout the data lifecycle.

5.3 **Protection / Confidentiality** – Appropriate levels of protection need to be in place to protect information assets that contain personal information and those that are confidential, privileged, or otherwise sensitive in nature. At the time of collection, the purpose for collection, and identification of how the information will be used (including the sharing of any data).

5.4 **Accountability** - An executive sponsor should oversee the IDG program and delegate responsibility for Information Management to appropriate individuals. The City adopts policies and procedures to guide personnel and ensure the program can be audited.

5.5 **Lifecycle Management** – Information should be retained as per the Records Retention By-law, and in accordance with legal, regulatory, fiscal, operational and historical requirements.

Information should be disposed of or transferred to the Archives when no longer required as outlined by the Records Retention By-Law. Disposition should occur in an appropriate and secure manner.

5.6 **Compliance** – Information should be managed to comply with applicable laws, regulations and other binding authorities, as well as City policies.

6. Mandatory Requirements

To create a standardized approach for managing all information assets, in a large and complex technical environment, in accordance with legislation, organizational policy and business goals and enable:

6.1 **Informed Decision Making** - Gain full understanding of all information and data the City requires to make informed business decisions.

6.2 **Risk Mitigation** – Prepare for and respond to audits, discovery and compliance, while mitigating or limiting exposure to risks such as privacy and security incidents and breaches.

6.3 **Managed Information and Data** – Ensure lifecycle management of information and data based on internal standards and policies that also control information and data usage, quality and lineage.

6.4 **Well-Managed Technologies** – Develop a robust, integrated approach to Data and Information Technology management so that new and updated solutions are built or acquired with governance in mind.

6.5 **Accountability and Transparency** - Provide the tools to deliver visible results to the public and staff, while improving accountability to taxpayers.

6.6 **Compliance** –Ensure all sensitive information and data is managed and organized in a way that enables the City to meet business rules, and legal and governmental regulations.

7. Roles and Responsibilities

7.1 **Corporate Leadership Team**

- The IDG program will be endorsed and promoted by the Corporate Leadership Team for successful adoption across the City.

7.2 Department Heads

- Are responsible for the creation, capture, quality, use, protection, retention, and disposition of all departmental records.

- Ensure their business processes comply with this Policy, and all information and data management best practices.

7.3 Elected Officials

- The IDG program will be endorsed and promoted by City Council for successful adoption across the City.

7.4 Employees

- Create accurate and reliable information assets to support business activities.

- Protect personal and confidential information throughout its lifecycle.

- Ensure records are captured, stored, and shared/transmitted using a City approved Recordkeeping System and/or technology.

- Ensure appropriate protection against unauthorized use, loss/theft of records.

7.5 Information and Data Governance Bodies

- **Information and Data Governance Executive Sponsorship Committee (IDGES):**

  The executive sponsorship team is made up of elected officials, the Corporate Leadership Team, and will be sponsored by the City Clerk and the Chief Information Officer. This team provides direction and approval for the IDG program.

  Specifically, the IDGES team will:

  - Approve the IDG framework.
  - Approve the strategic direction of the IDG program, including vision, goals and priorities.
  - Approve policies and standards for data governance across the corporation.
  - Approve funding and resource allocation to meet the strategic objectives.

- **Information and Data Governance Steering Committee (IDGSC):**

Define the strategic vision, goals, policies, procedures and more. This committee will set the priorities for the information and data initiatives. The IDGSC will be comprised of the following core teams: Information Management, Privacy, Information Technology, Insurance and Risk, Legal and the IDG Champion. The CAO's office and the Internal Audit Teams will be included as required.

- **Information and Data Governance Committee (IDGC):**

  Handles the day-to-day operations of the program. This committee is made up of representatives from each division/department, each of whom will act as Information and Data Stewards.

  The IDGC is the execution layer of the Information and Data Governance structure, responsible to ensure compliance with corporate information and data policies, standards & external regulation. IDGC reviews and approves Information and Data Governance and management standards. IDGC also prepares investment recommendations for IDGSC. This group is comprised of the Information and Data Stewards, who will be involved in various discussions at the IDGSC. These individuals are subject matter experts in their fields and will champion the initiatives and priorities within their division and/or section.

7.6 Information and Data Governance Team

- The Information and Data Governance Team is made up of individuals from both the Information Management and Information Technology Teams. This team works collaboratively with three governance bodies: the Information and Data Governance Executive Sponsorship Committee (IDGESC); the Information and Data Governance Steering Committee (IDGSC); and the Information and Data Governance Committee (IDGC).

- The oversight and management of all information within the City is centralized through the Information Management Team, under the City Clerks Office.

- The oversight and management of technology used by the City is centralized through the Information Technology Team.

7.7 Information and Data Stewards

- The Information & Data Steward is someone that ensures the information within their department stays accurate and up to date, ultimately improving efficiencies. They understand how departmental information and data is collected, maintained, used and interpreted.

- The Information & Data Steward is a function and not a unique and defined role within each department.

7.8 Information Management Team

- Accountable for the compliance with the Municipal Act and the Municipal Freedom of Information and Protection of Privacy Act, as they address records and information management.
- Provides leadership, direction, and vision for the City's overall Information Management program.
- Provides authority for Information Management processes, procedures, and methodologies and for approving contractors for Information Management services (digitization, shredding and storage).

7.9 Information Technology Team

- Monitor the use of IT resources to ensure compliance with corporate policies, administrative directives, and procedures.
- Establish hardware, software, video, and communications technology standards to ensure a secure and reliable information technology and communications environment.
- Implement tools such as firewalls, encryption, and antivirus software, as well as technology to identify potential security risks, discover sensitive data, monitor its activity, and prevent its loss.
- Monitor and report on health of the system.
- Support corporate accountability and transparency through programs such as Open Data.

8. Monitoring and Compliance

8.1 The IDG program will produce a variety of reports to monitor compliance with IDG rules. These reports will be reviewed by the Governing bodies and will be distributed to staff on occasion to aid in the correction of errors.

8.2 Periodic reviews of systems and repositories will occur to ensure that information assets are being managed in accordance with all policies, procedures and by-laws that form the Information and Data Governance Policy Framework.

8.3 Consequences of non-compliance

8.3.1 Failure to follow this Council Policy may result in:

- Breach or compromise of confidential or personal information.
- Inability to identify historical, vital, or business critical records.
- Loss of vital information.

- Inability to comply with legal requirements as outlined in the Records Retention By-law.
- Unclassified or misclassified information.
- Inability to find, use, re-use or leverage information due to poor controls.
- Poor data quality.
- Mismanagement of City assets.

9. Definitions

9.1 **Data** – Any symbols or characters that represent raw facts or figures and form the basis of information. Data is structured information.

9.2 **E-discovery** - E-discovery is a form of digital investigation that attempts to find evidence in corporate systems that could be used in litigation or criminal proceedings. The traditional discovery process is standard during litigation, but e-discovery is specific to digital evidence. The evidence from electronic discovery could include data from email accounts, instant messages, social profiles, online documents, databases, internal applications, digital images, website content and any other electronic information that could be used during civil and criminal litigation.

9.3 **Records and Information** – Any recorded information, regardless of media type or format, which documents the City of Brampton's business transactions, decisions, and activities.

9.4 **Information and Data Governance** - The Association for Records Managers and Archivists' (ARMA) Information Governance Body of Knowledge defines information governance as a "strategic, cross-disciplinary framework composed of standards, processes, roles, and metrics that hold organizations and individuals accountable for the proper handling of information assets."

9.5 **Information and Data Governance Strategy and Framework** – the process of managing the availability, usability, integrity and security of information and data stored in City systems, based on internal standards, policies, controls, and governance best practices.

9.6 **Information Asset** – information assets are bodies of information (records, data, content, knowledge, etc.), defined and managed as a single unit so they can be understood, shared, protected, and used efficiently. Information assets have recognizable and manageable value, risk, content and lifecycles.

9.7 **Information Lifecycle** – The major milestones of a record's existence, subject to changing requirements: creation/receipt, classification, use, retention, and disposition (i.e., transfer to another entity, archival retention, or destruction).

9.8 **Legacy System** – A legacy system is outdated computing software and/or hardware that is still in use. The system still meets the needs it was originally designed for but doesn't allow for growth. A legacy system is typically an older technology that won't allow it to interact with newer systems.

9.9 **Legal Hold** – Refers to a hold order or notice received by the City, which requires the City to preserve all forms of relevant information, as a result of reasonably anticipated investigations, access requests, audit or lawsuit. A legal hold suspends the normal disposition or processing of records.

9.10 **Master Data** - Is the core data that is absolutely essential for running operations within a business enterprise or unit. It is data about key business entities that provides context for business transactions and operations. Master data is needed by several business processes as well as their IT systems. Therefore, it is imperative to standardize master data formats, synchronize values, and manage data properly to bring about successful integration into the system.

9.11 **Privacy Breach** - means inappropriate collection, use or disclosure of personal information.

9.12 **Record** – any recorded information, regardless of medium or characteristics, made or received and retained by an organization in pursuance of legal obligations or in the transaction of business.

9.13 **Records Retention By-Law** - A legal document that lists the records that the City creates and receives with defined retention timeframes.

9.14 **Security Breach** - A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms.

10. References and Resources

This Council Policy should be read and applied in conjunction with the following references and resources as updated from time to time. Please note that some of the following documents may not be publicly available.

10.1 External references

- ARMA International
- DAMA International
- Information and Privacy Commissioner of Ontario

10.2 References to related bylaws, Council policies, and administrative directives

- Accountability and Transparency Policy
- Business Continuity AD
- Code of Conduct for Members of Council
- Electronic Monitoring
- Employee Code of Conduct
- Information Management AD

- Open Data Policy
- Privacy AD
- Records Retention By-law
- Use of Corporate Resources Policy
- Use of IT Resources AD

10.3 References to related corporate-wide procedures, forms, and resources

- Data Analytics Guidelines
- Data Matching Guidelines
- Data Sharing Guidelines
- GeoHub (Service Card)
- Governing Information and Data Service Card
- MFIPPA SOP
- MFIPPA Manual
- Privacy Impact Assessment SOP
- Privacy Incident Management SOP
- Sample Notice of Collection
- Self Service (Service Card)
- Web Analytics and Reports (Service Card)
- Technology Business Continuity and Recovery SOP

11. Revision History

Date	Description
yyyy/mm/dd	Next Scheduled Review *(typically three years after approval)*