BRAMPTON

COUNCIL POLICY

Category: Governance

Information and Data Privacy and Protection

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]

1. Background

The City of Brampton (“the City”) protects against the unauthorized access, use, corruption, disclosure, and distribution of non-public, corporately sensitive and/or personal information, and must comply with all applicable Federal and Provincial legislation and regulations regarding such information. The City shall hold sensitive and/or personal information in strict confidence and shall not release or disclose such information to any person except as required or authorized by law and only to such persons who are authorized to receive it.

The City shall ensure that any entity providing services to, or on behalf of the City, as well as any entity that utilizes information assets provided by the City to carry out its responsibilities, shall offer the same or higher levels of protection.

2. Purpose

The purpose of this Council Policy is to safeguard all personal and sensitive information and data that is stored by the City of Brampton, including on-premises, offsite locations, and cloud services. Personal and sensitive information may include citizen, visitor, business, and City employee information. Information assets must be protected in a manner that maintains public trust. At the same time, Protections must also comply with Federal, Provincial, Regional, and Municipal legislation as well as other national and international regulations, standards, and best practices.

3. Application and Scope

This Council Policy applies to all departments and units under the jurisdiction of the City, including:

- All employees including full-time, part-time, contract, temporary employees, elected and appointed officials, volunteers, co-op students, and any other individuals who perform work on behalf of the City.
- Third parties such as contractors, vendors, partners, and other entities that handle or process data on behalf of the City or have access to the City's data.

Scope:

- All Personally Identifiable Information (PII)
- Corporately Sensitive Information Assets
- Information and data lifecycles
- Digital and physical records
- All IT systems, applications, software, hardware, networks, databases, cloud platforms, and other technology assets used by the City and Councillors to process data.

3.1 Exceptions

3.1.1 This Council Policy does not apply to the content of Political Information assets of Councillors.

4. Outcomes

There are a range of positive outcomes with tangible and intangible benefits:

4.1 **Enhanced Public Trust**: By demonstrating that the City values and actively protects the personal data of its citizens, public trust in city management and its digital services will be reinforced.

4.2 **Compliance with Regulations:** The City would be in alignment with provincial, federal and potentially international data protection regulations, thereby avoiding legal repercussions, fines, and sanctions.

4.3 **Reduced Risk of Breaches**: With proper data protection measures in place, the likelihood of data breaches diminishes, safeguarding the city against financial, reputational, and operational damages.

4.4 **Clear Data Management:** The policy can lead to more organized, streamlined, and efficient data management processes, allowing the city to make better data-driven decisions.

5. Principles

5.1 **Accountability** – The City is responsible for personal information under its care and control and shall designate an individual or individuals who are accountable for the organization's compliance with these principles.

5.2 **Identifying Purpose** - The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

5.3 **Consent** - The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

5.4 **Limiting Collection** - The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

5.5 **Limiting Use, Disclosure, and Retention** - Personal Information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

5.6 **Accuracy** - Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

5.7 **Safeguards** - Personal Information shall be protected by security safeguards appropriate to the sensitivity of the information.

5.8 **Openness** – The City shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

5.9 **Individual Access** - Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

5.10 **Confidentiality -** Information is only being seen or used by people who are authorized to access it.

5.11 **Integrity -** This principle guarantees the integrity and accuracy of data and protects it against modifications. This means that any changes to the information by an unauthorized user are impossible (or at least detected), and changes by authorized users are tracked.

5.12 **Availability -** This principle ensures that the information is fully accessible at any time whenever authorized users need it, and that all the systems used to store, process, and secure all data must be functioning correctly.

5.13 **Challenging Compliance** - Individuals shall be able to challenge the City's compliance with these principles, and the City shall designate staff who will be accountable for responding to such challenges.

6. Policy Statements

6.1 **Lawfulness, Fairness, and Transparency**: Information and data should be processed lawfully, fairly, and in a transparent manner.

6.2 **Purpose Limitation**: Information and data should be collected for specific, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. The City shall not collect more personal information than is required to provide its programs and services.

6.3 **Data Minimization**: Information and data collection should be relevant, limited, and adequate to what is necessary for the purposes for which it is processed.

6.4 **Consent**: Where applicable, information and data should only be processed when explicit consent has been given by the data subject, where possible, and this consent can be withdrawn at any time. Where explicit consent cannot be obtained, a notice of collection is provided in advance of the collection.

6.5 **Integrity and Confidentiality**: Information and data should be processed securely, ensuring protection against unauthorized or unlawful processing, accidental loss, destruction, or damage.

6.6 **Information Asset Protection by Design and Default**: Information and data protection should be included from the onset of the design of systems, rather than as an addition or after-thought.

6.7 **Accuracy**: Personal information and data should be accurate and, where necessary, kept up to date. Inaccurate data should be erased or rectified without delay.

6.8 **Training and Awareness**: All staff involved in information and/or data processing should be trained and aware of their responsibilities and obligations regarding data protection.

6.9 **Risk Assessment**: Before starting projects that process personal or sensitive data, an assessment of the potential risks and impacts on information asset protection should be conducted.

6.10 **Information Asset Protection**: Staff, contractors and volunteers who may handle personal information or confidential information must be aware of, and comply with, legislated requirements and established best practices related to privacy and security. The City will make every reasonable effort to prevent any loss, misuse, disclosure, or modification of personal information. Appropriate physical and digital security measures will be employed to protect records that contain personal information and to prevent inappropriate use.

6.11 **Information Asset Retention**: Personal information will be retained only for as long as necessary to fulfil the stated purpose as identified in the Records Retention By-Law.

6.12 **Information Correction**: Individuals have a right to access their own Personal Information in a record that is in the custody or under the control of the City, subject to legislated exceptions. Individuals may also request information about the City's use of their Personal Information and any disclosure of that information to persons outside the City.

7. Roles and Responsibilities

7.1 Access and Privacy Coordinator

- Develops and delivers privacy-related training.
- Coaches and provides privacy-related advice to staff and elected officials.
- Conducts Privacy Impact Assessments.
- Updates Personal Information Banks.
- Initiates the privacy breach protocol and investigates suspected privacy breaches.

7.2 Corporate Leadership Team

- The Privacy and Security programs will be endorsed and promoted by the Corporate Leadership Team for successful adoption across the City.

7.3 Department Heads

- Are responsible for the creation, capture, quality, use, protection, retention, and disposition of all departmental information assets.
- Ensures their business processes comply with this Policy, and all information and data management best practices.

7.4 Elected Officials

- The security and privacy programs will be endorsed and promoted by City Council for successful adoption across the City.

7.5 Employees

- Protects personal and confidential information throughout its lifecycle.
- Ensures records are captured, stored, and shared/transmitted using a City Approved Recordkeeping System and/or technology.
- Ensures appropriate protection against unauthorized use, loss/theft of records.

7.6 Information and Data Governance Bodies

7.6.1 Information and Data Governance Executive Sponsorship Committee (IDGES):

- Composed of elected officials, the Corporate Leadership Team, and is sponsored by the City Clerk and the Chief Information Officer. Provides direction and approval of the Information and Data Governance (IDG) program, including approval of policies and standards for information and data governance across the corporation.

7.6.2 Information and Data Governance Steering Committee (IDGSC)

- Defines the strategic vision, goals, policies, procedures and more. This committee will set the priorities for the information and data initiatives.

7.6.3 Information and Data Governance Committee (IDGC)

- Ensures compliance with corporate information and data policies, standards & external regulation.

7.7 Information and Data Governance Team

- Comprised of individuals from 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 Clerk's Office.
- The oversight and management of technology used by the City is centralized through the Information Technology Team.

7.8 Information and Data Stewards

- Ensure the information within their department stays accurate and up to date, ultimately improving efficiencies. They understand how departmental information and data is secured and protected.

7.9 Information Management Team

- Accountable for 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, including access to information and privacy.

7.10 Information Technology (IT) 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.

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 and protected in accordance with all policies, procedures and by-laws that form the Information and Data Governance Policy Framework.

8.3 Periodic reviews will be conducted by Internal Audit and reported on to the Internal Audit Committee.

8.4 Consequences of non-compliance

Failure to follow this Council Policy may result in a privacy breach and/or prosecution of a Provincial or Federal offence. The consequences of a privacy breach may include reputational damage to the City, negative publicity, litigation and financial damages. The City's response to a privacy breach focuses on limiting any damages arising from the breach and on changing systems to prevent future breaches. City employees acting in good faith and in compliance with this Council Policy will not be subject to disciplinary action for privacy breaches. Failure to adhere to the provisions in this Policy will result in a review of the circumstances by Human Resources and Corporate Leadership, and if a failure is validated, will result in disciplinary action.

The consequences of conviction of a Provincial or Federal offence may include a fine, reputational damage to the City and reputational damage to affected staff. The legislation provides that staff acting in good faith and to the best of their abilities will not be subject to prosecution. Negligence or willful violation of legislation may result in prosecution of staff and/or the City.

9. Definitions

9.1 **Approved Recordkeeping System**, AKA Information Management System – a system (manual or electronic) that captures, controls and provides access to records over time, as the content moves through the Information Lifecycle.

9.2 **Core Infrastructure** –The combined components of your business' computer network, which at its core includes servers, switches, and storage, whether on premise or hosted in a Cloud platform.

9.3 **Corporately Sensitive Information Assets** – Sensitive business information includes anything that poses a risk to the company in question if discovered by an unauthorized person. This information may include draft by-laws, closed meeting minutes, advice to other levels of government, legal enforcement information, labour relations records, etc.

9.4 **Information Asset** – An information asset is a collection of records, information, data, knowledge, or content that relates to business activities, that is organized, managed, and valuable.

9.5 **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).

9.6 **Personal Information** - Depicts any recorded information about an identifiable individual. The City uses the meaning specified in the *Municipal Freedom of Information and Protection of Privacy Act*.

9.7 **Personal Information Bank** This refers to a collection of records that contain personal information that can be searched and accessed using a person's name, an identifying number or other identifier. The City uses the meaning specified in the *Municipal Freedom of Information and Protection of Privacy Act*.

9.8 **Personally Identifiable Information** – This refers to any recorded information about an identifiable individual. The City uses the meaning specified in the *Municipal Freedom of Information and Protection of Privacy Act*.

9.9 **Political Information** - Political information refers to information and records that document a Councillor's relationship with their constituents and are considered the personal property of the Councillor.

9.10 **Privacy Breach** - Means inappropriate collection, use or disclosure of personal information.

9.11 **Privacy Impact Assessment** – Depicts a formal assessment of privacy obligations, risks, and requirements related to a given program, technology, service, or personal information bank.

9.12 **Security Breach** – This refers to any incident that results in unauthorized access to data, applications, services, networks, and/or devices by bypassing their underlying 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
- Municipal Freedom of information and Protection of Privacy Act

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

- Electronic Monitoring Administrative Directive
- Information Management AD
- Privacy AD
- Retention By-law
- Technology Business Continuity and Recovery SOP
- 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
- Governing Information and Data Service Card
- MFIPPA SOP
- MFIPPA Manual
- Personal Information Banks
- Privacy Impact Assessment SOP
- Privacy Incident Management SOP
- Sample Notice of Collection

11. Revision History

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