Information Management Standard – Information Protection Classification Standard

Standard No.: CIMS-S003
Version No.: 1.0
Issued On: March 6, 2023
Issued By: Corporate Information Management Services, City Clerk's Office
Subject: information management
Keywords: data sensitivity, classification, protection, records management

Foreword: City of Toronto Information Management Policies and Standards are the official publication on the policies, standards, directives, guidelines, position papers and preferred practices given oversight under delegated authority of Toronto Municipal Code, Chapter 217, Records, Corporate (City). These publications support the City's responsibilities for coordinating standardization of Information Management in the City of Toronto.

Acknowledgements: This Standard acknowledges the efforts, subject matter expertise, and oversight provided by the following:

- **Project Sponsor:** Kristie Pratt Deputy City Clerk, Corporate Information Management Services
- **Divisions & Business Units:**
  - **Corporate Information Management Services**
  - **Technology Services Division**
  - **Office of the Chief Information Security Officer**

Contact Information:
Kristie Pratt
Deputy City Clerk
Corporate Information Management Services, City Clerk's Office
City Hall, 13th floor, West Tower
100 Queen Street West
Toronto ON M5H 2N2
Tel: (416) 803-9140
Kristie.Pratt@toronto.ca

Table of Contents

1. Introduction

City of Toronto staff have a duty to uphold the confidentiality, integrity, and accessibility of City records. Building and maintaining public trust requires that our decisions about internal and external access to information align with information management, privacy and access best practices, policy, and legislation.

Decisions about how to grant access to a record are influenced by the nature of the information contained in the record and the purpose for which that information was collected or created. Failure to protect City records from unauthorized access or disclosure could result in real harm to the City, its staff, and to individuals to whom the information pertains.

The Information Protection Classification Standard is a document that defines categories and criteria to classify City records in line with the City's requirements for managing privacy. Determining and applying information protection classifications further promotes the implementation of proper safeguards and controls required for storage, access, disclosure, and processing of City records.

Within the City's context, privacy and access requirements are informed by our governing privacy legislation: the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and the Personal Health Information Protection Act (PHIPA). The categories of information in this Standard align to information types defined in this governing legislation. Related policies, including Information Management Accountability Policy, the Protection of Privacy Policy, and the Acceptable Use Policy, define the roles and responsibilities required to enable our legislation. In turn, this Standard provides a mechanism to classify records stored in City systems, repositories, and applications, in order to apply privacy protections commensurate to their sensitivity.

2. Purpose

The purpose of the Standard is to define information protection categories that ensure that all City staff and Divisions apply a consistent approach to classifying information and determining information protection requirements.

The Standard defines:

- What information protection categories can be applied to City records
- How to assess and identify which information protection category is appropriate for City records
- How to apply an information protection category
- Who is responsible for determining appropriate classification

This Standard is aligned with the Information Management Framework (IMF) and the Digital Infrastructure Strategic Framework (DISF). Use of this Standard contributes to the City's commitment to fostering a well-run City, which includes the effective management of information to:

- Ensure compliance with recordkeeping and privacy legislation
- Protect personal and sensitive information collected by the City of Toronto
- Support access to information to increase business efficiency
- Increase public access to records and information
- Improve the City's transparency and accountability
- Improve the accuracy of business intelligence and analytics activities to inform decision-making

3. Application

This Standard applies to all City of Toronto Divisions, City employees, volunteers, and third parties who access, create, store, and use records, data, and information on behalf of the City. Its application is effective for implementations beginning following its approval.

This Standard is intended for use by staff in roles that involve:

- receiving, creating, or editing City records
- assessing information systems, repositories, and applications
- developing systems to collect, process, disclose, and manage records
- managing internal user permissions and access to records
- protecting records from unauthorized access or use
- processing requests for public access to information

This Standard does not apply to:

- **Elected Officials**
  Disclosure of Elected Officials' information is at the discretion of the appropriate Elected Officials.

- **Accountability Officers**
  The City's Accountability Officers include the Auditor General, Integrity Commissioner, Lobbyist Registrar, and Ombudsman. The City of Toronto Act requires that the Officers independently perform their duties and establish confidentiality requirements for their information.

  These confidentiality requirements are recognized in Toronto Municipal Code Chapter 3, Accountability Officers, and the City's Protection of Accountability

Officers' Information Directive developed to safeguard the confidentiality of the Officers' information.

- **Agencies and Corporations**
  The City of Toronto encourages City Agencies and Corporations to review, adopt, or update this Standard as appropriate to their business needs

4. Scope

This Standard addresses City records, information, and metadata created or received during City administration or delivery of City services. It applies to physical and electronic records and information. This Standard applies in situations where records, information and metadata are created, processed, transmitted, or stored by a third party or contractor. Records created by the Mayor's Office are considered City records and are subject to this Standard.

The application of information protection categories is determined by point-in-time review of information systems, repositories, and applications, in context of the types of records and information they are intended to store, and the privacy and security features they offer. As the City of Toronto matures in applying this Standard, additional guidance may be developed to provide best practices for technology protections mapped to the six classification categories.

Appropriate privacy controls must be implemented to secure City records, information systems, and other resources to a degree that is consistent with the principles outlined here or as may be outlined in other City of Toronto policies and legislation. Additional safeguards for information systems may also be recommended in a Privacy Impact Assessment, Threat Risk Assessment, Risk Treatment Plan, Risk Mitigation Plan, or other documents that identify risks to the integrity and security of City records.

5. Information Protection Principles

Principle 1: Proper Application

All records, data, and information collected, created, or processed during City business and administration, regardless of format, is subject to classification based on the level of protection it requires.

- This Standard outlines six information protection classifications:
  - **Public Information**: records that are available to the public without restriction.
  - **Routinely Disclosed Information**: records that can be released without a Freedom of Information Request.
  - **Exempt For Review Information**: records that are exempt under Part 1 of MFIPPA.

  - **Excluded Information**: sensitive or confidential information that has restrictions on its access.
  - **Personal Information:** recorded information about an identifiable individual.
  - **Personal Health Information**: identifying information about an individual that is in the custody or control of a Health Information Custodian**.**

- Any information that has not undergone a classification exercise must be treated as exempt by default. Disclosure of exempt information to the public requires a Freedom of Information (FOI) request and review by the City Clerk's Office's Access Unit. Disclosure to other City Divisions requires a review and classification of the information by its owner.
- Excluded information is not subject to the access provisions set out in MFIPPA, and the information owner shall refuse disclosure of such information until it is reviewed for personal information, personal health information, or other confidential information that should not be disclosed to the public. Excluded information may be disclosed on a discretionary basis, subject to Divisional policy.
- Transitory records may be subject to classification, depending on their context and storage location.
- Multiple protection classifications can be applied to information. For example, many routinely disclosed records from Court Services also contain personal information. The information protection classification that is least permissive shall, with limited exception, take precedence for classification and configuration of privacy protections.
- Integration of information sources (e.g., aggregation or joining of various datasets) can impact the classification of the underlying information as it may reveal new information about an individual or incident with privacy implications. Aggregated records are considered a separate record for the purpose of classification.

Principle 2: Privacy by Design

Information protection categories are applied by design to City systems, repositories, and applications.

- Information protection classification by-design is the process of systematically integrating information protection classification into divisional business practices and technology system design and implementation.
- Information protection classification is applied as broadly as possible to information sources, such as systems, applications, and repositories. This “top-down” classification approach provides comprehensive safeguards for all the records stored and managed within those technologies.

- Information protection should be assessed and enabled whenever a new system, application, or repository is implemented. Corporate Information Management Services (CIMS - City Clerk's Office) performs an IM Assessment of new technologies to ensure information is classified and appropriate technology protections are planned for. Divisions are then accountable for ensuring that information is protected commensurate to its classification and applicable legislation.
- Following the above, classifications applied to systems, repositories, and applications should be reviewed regularly by the Division that stewards the records, as well as the staff who administer the system, repository, or application that stores the records.
- Staff are not responsible for applying information protection classifications directly to individual documents or records, with limited exceptions.

Principle 3: Divisional Enablement

Information protection classification is enabled on a Divisional basis.

- City Divisions, in collaboration with CIMS, are responsible for determining what information protection classification is appropriate for the records and information they own, consistent with the purposes for which the information was collected, as well as their Divisional business needs.
- Division Heads are responsible for protecting personal privacy in the records and information they create and steward.
- Re-classification of a record is at the discretion of the Division that stewards the record.
- City Divisions must ensure staff, including employees, contractors, and third parties maintain a level of privacy and information protection awareness appropriate with their responsibilities.
- City Divisions inform staff, including employees, contractors, and third parties of the legal and administrative consequences of inappropriate or unauthorized access to, or collection, use, or disclosure of City records and information.

Principle 4: Shared Responsibility

All staff who work with City information, including City employees, contractors, and third parties, are responsible for safeguarding the information they create, collect, and access.

- Division Heads delegate authority to their staff to apply information protection classifications as appropriate to their business context.
- Staff should not share or distribute records and information that do not have an information protection classification.

6. Information Protection Classification Categories

Classification Categories	Public Information	Routinely Disclosed Information	Exempt-for-Review Information	Excluded Information	Personal Information	Personal Health Information
When to use this Classification	Applies to records that are available to the public without restriction and can be accessed without a Freedom of Information request or routine disclosure request. This includes: 1. Records expressly created, collected, or curated in order to be made available to the public, such as Open Data and archival records. 2. Personal Information that is mandated to be publicly available under section 27 of MFIPPA, such as property assessments. 3. Published information that is subject to section 15 of MFIPPA, such as City Council reports.	Applies to certain operational and administrative records that can be released without a Freedom of Information Request. Records that can be routinely disclosed are identified in divisional Routine Disclosure Plans. Routinely Disclosed Information must be reviewed and identified by a Division or Health Information Custodian prior to disclosure.	Applies to records that are exempt under Part 1 of MFIPPA. Exemptions include: 1. draft by-laws 2. advice or recommendations 3. law enforcement records 4. records regarding relations with governments 5. records regarding relations with Aboriginal communities 6. third party information 7. records regarding economic and other interests 8. solicitor-client privilege 9. danger to safety or health 10. personal privacy 11. information soon to be published Records that do not have an information protection classification are considered **exempt by default** to reduce risks around handling, storage, and disclosure until the records can be reviewed and classified appropriately.	Applies to sensitive or confidential information that has restrictions on its access, including: 1. employment-related information 2. labour relations or negotiations information, subject to the exceptions identified in MFIPPA s.52(4) 3. information relating to a legal prosecution case initiated by the City of Toronto 4. archival records acquired from private donors that are subject to access restrictions 5. information that is critical to the delivery of City services and infrastructure 6. identifying information in a record relating to medical assistance in dying. Neither the public, nor the individual to whom the information relates have general rights to Excluded Information. Neither the privacy provisions nor the access rights of MFIPPA apply.	As defined in MFIPPA, “personal information” means recorded information about an identifiable individual, including: 1. information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual 2. information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved 3. any identifying number, symbol or other particular assigned to the individual 4. the address, telephone number, fingerprints, or blood type of the individual 5. the personal opinions or views of the individual except if they relate to another individual 6. correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence 7. the views or opinions of another individual about the individual 8. the individual’s name if it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual	As defined in PHIPA, this applies to identifying information about an individual in oral or recorded form that is in the custody or control of a Health Information Custodian, if the information: 1. relates to the physical or mental health of the individual, including information that consists of the health history of the individual’s family 2. relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual 3. is a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual 4. is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the Connecting Care Act, 2019 5. relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual 6. relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance 7. is the individual’s health number, or 8. identifies an individual’s substitute decision-maker
Accountability	City Officials, including Division Heads and their designates are accountable for identifying and applying information protection categories to City systems, repositories, and applications.					
Classification	Information protection classification categories are applied “by design” to City systems, repositories, and applications. Classifications are inherited by the records stored within those systems, repositories, and applications wherever possible. Classification protections and configurations will be dependent upon which functionalities are available within a given system.					
Labeling	As evidence of having been classified, information systems, repositories, applications, and/or records shall be marked with one of the six information protection categories described above. The type of marking or labelling will be dependent on the capabilities of the solution housing the records, as well as the format and medium of the records. Labels may take the form of a visual marking, such as a watermark, stamp, or GUI component, or as metadata.					

7. References

The following sources were used in the development of this Standard:

Legislation

- Province of Ontario (2021). Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). Retrieved from: https://www.ontario.ca/laws/statute/90m56
- Province of Ontario (2021). Personal Health Information Protection Act (PHIPA). Retrieved from: https://www.ontario.ca/laws/statute/04p03
- City of Toronto, Legal Services (2022). Municipal Code Chapter 217, Records, Corporate (City). Retrieved from: http://www.toronto.ca/legdocs/municode/1184_217.pdf

Policies and Standards

- City of Toronto, City Clerk's Office (2018). Information Management Accountability Policy. Retrieved from: https://www.toronto.ca/wp-content/uploads/2018/07/8ec6-information-management-accountability-policy.pdf
- City of Toronto, City Clerk's Office (2019). Protection of Privacy Policy. Retrieved from: https://www.toronto.ca/wp-content/uploads/2022/06/9097-Protection-of-Privacy-Policy2022approved.pdf
- City of Toronto, Office of the Chief Information Security Officer (2021). Access Control Standard. Retrieved from: http://insideto.toronto.ca/itweb/policy/pdf/access-control.pdf
- City of Toronto, Office of the Chief Information Security Officer (2021). Cloud Security Policy. Retrieved from: http://insideto.toronto.ca/ciso/files/cloud-security-policy.pdf
- City of Toronto, Office of the Chief Information Security Officer (2021). Cyber Security Policy. Retrieved from: http://insideto.toronto.ca/ciso/files/cyber-security-policy.pdf
- City of Toronto, Technology Services Division (2018). Acceptable Use Policy. Retrieved from: http://insideto.toronto.ca/itweb/policy/pdf/acceptable_use.pdf

8. Approval

Approval provided by Deputy City Clerk Kristie Pratt, effective March 6, 2023.

9. Standard Review

The City Clerk's Office will review this Standard and its effectiveness two years from the effective date of this Standard, or earlier if warranted.

Appendix A: Definitions

Application: An application, also referred to as an application program or application software, is a computer software package that performs a specific function directly for an end user or, in some cases, for another application. An application can be self-contained or a group of programs

Classification: An activity comprised of grouping similar or related things (concepts or terms) together; separating dissimilar or unrelated things; and arranging the resulting groups into a logical sequence.

City Official: The employee, responsible for information created, collected, or processed on behalf of the City of Toronto.

City Record: Recorded information created or received in the course of City administration or delivery of City services.

Excluded Information: Sensitive or confidential information that falls outside the authority of MFIPPA, and is subject to discretionary access restriction. Neither the public, nor the individual to whom the information relates have general rights to Excluded Information. Neither the privacy provisions nor the access rights of MFIPPA apply to excluded information.

Exempt Information: Information that falls outside of the general right of access outlined in MFIPPA. Exemptions may be discretionary or mandatory, depending on the nature of the information.

Freedom of Information Request: A formal request for records of the City of Toronto under the access provisions of MFIPPA.

Health Information Custodian: A person or organization listed in PHIPA that, as a result of his, her or its power or duties or work set out in PHIPA, has custody or control of personal health information.

Personal Health Information: Personal health information is defined as identifying information about an individual in oral or recorded form, that is in the custody or control of a Health Information Custodian, if the information:

- relates to the physical or mental health of an individual, including information that consists of a person as a provider of health care to the individual
- relates to the providing of health care to the individual including identification of a person as a provider of health care (e.g., physician's name) to the individual
- is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual
- relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual
- relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance
- is the individual's health number, or identifies an individual's substitute decision-maker
  For more information, refer to the Definitions section under PHIPA, S.2.

Personal Information: Personal information is recorded information about an identifiable individual, such as (but not limited to):

- address
- race, religion, gender, family status
- employment history
- medical history, blood type, DNA
- any identifying number assigned to the individual
- personal opinions or views of an individual about another individual
- correspondence of a personal or confidential nature from an individual
  For more information, refer to the personal information interpretation under MFIPPA, S.2

Privacy: The right to be let alone; assurance that the confidentiality of, and access to, certain information about an entity is protected.

Repository: A centralized place where data is stored and maintained in an organized way.

Routine Disclosure: The routine or automatic release of certain types of administrative and operational records in response to informal rather than formal requests under the Municipal Freedom of Information and Protection of Privacy Act.

Security: The practice of defending computers, servers, mobile devices, electronic systems, networks, information and data from malicious attacks, compromise, or theft. It can also be known as IT security, electronic information security or information security.

Cyber security is defined in terms of confidentiality, integrity, availability, identification, authentication, authorization, and non-repudiation.

System: A discrete set of resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information

Appendix B: Authority – Legislative Analysis

City records are open by default, with restrictions being the exception, not the rule. The Information Protection Classification Standard is based on the following premises:

1. Internal and external information security
MFIPPA Regulation 823, Section 3 defines the primary legal requirements of institutions subject to the Act:

- 3 (1) Every [Institution] head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented, and put in place, taking into account the nature of the records to be protected.
- 3 (1).(2) Every [Institution] head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.
- 3 (2).(3) Every [Institution] head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented, and put in place, taking into account the nature of the records to be protected.

Records that have access restrictions must maintain a level of information security internally, while also preventing external disclosure. In practice, this can often be applicable even within an office between co-workers. The premise may be summed up by applying the adage that "if you don't need the file for your job, you don't get to see it."

2. Records are exempt for review by default
MFIPPA Section 1 states: The purposes of this Act are:
(a) to provide a right of access to information under the control of institutions in accordance with the principles that,
(i) information should be available to the public,
(ii) necessary exemptions from the right of access should be limited and specific.

The exemptions are described in sections 6 to 15 of MFIPPA, Part 1. Of these exemptions, only three are considered mandatory:

- Section 9, Relations with Other Governments
- Section 10, Third Party Information
- Section 14, Personal Information

The other exemptions are discretionary. Records that have not been classified, or otherwise been made available as public records or through routine disclosure must first be reviewed by City Clerk's Office staff, subject to a formal Freedom of Information (FOI) request, prior to disclosure.

3. Records excluded under MFIPPA

This classification framework also considers MFIPPA Section 52, Application of the Act. These records are deemed to fall outside of MFIPPA and are governed by internal City of Toronto policies and best practices. Excluded documents include employment-related records maintained by the City, as well as archival records acquired from private donations subject to access restrictions. Access to excluded information is discretionary and determined by the Divisional owner of the information.

4. Records excluded under PHIPA

Health Information Custodians (HICs) within the City of Toronto, including Senior Services and Long-Term Care, Toronto Public Health, and Toronto Paramedic Services legislated by the Personal Health Information Protection Act (PHIPA), not MFIPPA. PHIPA provides explicit limitations and requirements for the collection, use, and disclosure of Personal Health Information (PHI), with disclosure being the exception. The classification of information associated with medical treatment and care held by an HIC has the highest legal risk and disclosure of PHI has the highest formal legal and financial penalty under law comparatively. PHI warrants its own classification.