Privacy Impact Assessment Policy

Policy No.: No. CIMS-004
Version No.: No. 3.0
Approval date: July 27, 2023
Division: City Clerk's Office
Issued On: July 27, 2023
Subject: Protection of privacy
Keywords: privacy impact assessment, privacy, personal information, personal health information, PHI, PI, PII

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 policy acknowledges the efforts, subject matter expertise, and oversight provided by the following:

Project Sponsor: **Kristie Pratt** Deputy City Clerk, Corporate Information Management Services, City Clerk's Office

Divisions and Business Units:

- Office of the Chief Information Security Officer, Digital Rights Protection
- Technology Services Division

Revision History:

Version #	Version Date	Issued by	Changes in Document
2.0	2013-02-28	City Clerk's Office	Stronger authority language and clarification of roles and responsibilities.
2.0	2019-08-22	City Clerk's Office	Application Statement updated
3.0	2023-07-27	City Clerk's Office	Updated Requirements for a PIA section; updated roles and responsibilities; added monitoring and compliance appendix

Contact Information:

Kristie Pratt
Deputy City Clerk
City Clerk's Office, Corporate Information Management Services
City Hall, 13th floor, West Tower
100 Queen Street West. Toronto ON M5H 2N2
Tel: (416) 392-9673
Email: Kristie.Pratt@toronto.ca

Table of Contents

1. Introduction

The City of Toronto is responsible for ensuring the protection of individuals' privacy at all times. The protection of privacy also forms part of the City's Accountability and Openness principles as stated in the Information Management Framework. The City's Digital Infrastructure Strategic Framework (DISF) also defines Privacy and Security as a core principle. These principles identify the public's expectation of access to the City's information and the protection of their personal information.

Under the Toronto Municipal Code, Chapter 169, the City Clerk shall set objectives for the management of information in the City and is delegated the powers and duties of the Head of Privacy set out in the Municipal Freedom of Information and Protection of Privacy Act (MFIPPA). These duties and powers give the City Clerk authority to ensure reasonable measures are in place to protect personal information in the City's custody or control. The Protection of Privacy Policy defines roles and responsibilities for the collection, use, and management of personal information. It is the responsibility of all City staff to ensure these protections are in place within technologies, systems, programs, or services.

A privacy impact assessment (PIA) is an in-depth review and analysis of a project, program, technology system, and/or process and is intended to identify and resolve privacy risks throughout the design or redesign of a technology, system, program, or service.

Staff should be aware that there are consequences for not properly managing the City's information as a corporate asset, including privacy breaches, identity theft, fraud, loss of trust by the public, and legal action. Improperly managing personal information may result in financial penalties imposed by the Information & Privacy Commissioner of Ontario.

2. Purpose

The purpose of this Policy is to identify the City's responsibilities relating to privacy impact assessments, and to reassure the public that the City builds privacy protecting measures into its services, technologies, and systems.

3. Application

This Policy applies to all City Divisions; additionally, the Policy applies to any Health Information Custodians that have designated the City Clerk as their Institution's Head of Privacy.

This Policy applies to all City of Toronto employees, volunteers and contract employees hired by the City of Toronto.

This Policy does not apply to Elected Officials, Accountability Officers, or City Agencies, Boards and Corporations. The City of Toronto encourages City Agencies, Boards and Corporations to review, adopt or amend this Policy's principles as appropriate to their business circumstances.

4. Policy Statement

The City of Toronto will:

- Protect the privacy of individuals when personal information is collected, used, disclosed, or retained.
- Ensure that Divisional and enterprise projects provide the necessary resources (financial, technical and staff) to collect, use, retain, protect, and disclose personal information in compliance with applicable privacy legislation.
- Complete privacy impact assessments on all new services, technologies, and/or systems that involve personal information as identified during the PIA screening process.
- Ensure that Divisional and enterprise projects are aware of privacy risks so that they can take the necessary measures to mitigate those risks or make informed decisions about accepting risks.
- Develop risk mitigation responses to address priority privacy risks identified in PIA Reports.
- Use discretion to pause any projects that are not in compliance with this Policy.

5. Organizational Outcomes

By implementing and complying with this Policy, it is expected that the City will:

- Protect the personal information that it has under its custody and control.
- Be protected from potential harms, including financial or reputational harms.
- Comply with applicable privacy legislation.
- Reduce the risk of privacy breaches, data leakage, and other privacy-related incidents.
- Embed privacy-by-design principles into new systems and services.
- Reduce long-term costs related to privacy management.
- Promote awareness of privacy within the City.
- Improve data quality.

6. Requirements for a Privacy Impact Assessment

The Office of the Chief Information Security Officer (Office of the CISO) determines if a privacy impact assessment report (PIA Report) is required for a technology, system, program, or service, following a screening process with Divisions and enterprise projects, and submission of the privacy impact assessment form (PIA Form).

A PIA Report may be required in one or more of the following scenarios:

1. New or altered collection of personal information.
2. A shift from direct to indirect collection of personal information.
3. New data matching or increased sharing of personal information between programs within the same Division or across the City of Toronto. Digital service delivery initiatives may involve shared service delivery models where data is shared with more than one program area.
4. New data matching or increased sharing of personal information between the City and other government organizations or third parties.
5. Existing programs and systems are being consolidated, re-engineered and/or involve changes in functionality (e.g., linking to other databases with personal information about the same individuals to create a new client profile), providing a new set of users with access to information or technology.
6. Proposals that may affect client privacy in the collection, use, disclosure and/or retention of personal information.
7. Proposals involving innovative use of technologies or organizational solutions, for example, systematic public monitoring, Internet of Things (IoT) devices, use of machine learning to automate decision making, or novel reuse of personal information.
8. Purchasing new technology that may collect personal information.
9. Submitting the required documentation (business case, ITAPP Form) to purchase new software and/or hardware that may collect personal information (e.g., biometric fingerprint scanner/reader).
10. Proposed use of data warehouses, data farms, or data lakes.
11. Procurement of Software as a Service (SaaS) and other cloud-based technology solutions.
12. Planned changes to policies, business processes or systems that may separate personal information from other information within a system.
13. Proposed changes to security mechanisms used to manage and control access to personal information (e.g., granting citizens electronic access to their own information, digital identity solutions).

6.1 Documenting Risk

PIA Reports identify privacy risks and offer recommendations to address those risks. PIA Reports are not shared with the Division Head by default. Division Heads may request a copy of the PIA Report from the Office of the CISO.

Instead, the Office of the CISO offers Risk Treatment Plans (RTPs) that combine privacy risks and recommendations from the PIA Report with risks and recommendations identified from other cyber assessments. The RTP is provided to the appropriate risk owner.

For more information on RTPs please contact the Office of the CISO (CISO@toronto.ca).

7. Roles & Responsibilities

7.1 City Manager will:

- Ensure compliance with the Privacy Impact Assessment Policy.

7.2 Deputy City Managers will:

- Ensure this Policy is communicated to all staff, implemented, and enforced.
- Ensure information is shared and accessible to the greatest extent possible, while respecting security and privacy requirements.

7.3 City Clerk will:

- Lead development, monitoring, implementation, and compliance with this Policy.
- Support City Divisions and Project Sponsors in complying with this Policy and privacy legislation.
- Raise awareness of the PIA Policy and ensure the PIA Policy and PIA-related guidance and/or training documentation are communicated and made accessible to City of Toronto staff, in collaboration with the Office of the CISO.
- Individually, or jointly with the Chief Technology Officer, and Division Head or Project Sponsor, review the PIA Report and documented risks prior to implementation of any technology, system, program, or service involving the collection or use of personal information or personal health information.
- Individually, or jointly with the Chief Technology Officer, will use their discretion to pause any technology, system, program, or service where privacy compliance issues have not been addressed in a manner that satisfies the privacy risks raised in the PIA Report.
- Consult with the Division Head, Project Sponsor, and City Manager regarding any projects that pose significant privacy risks at a corporate level.
- Provide records and information management oversight and guidance on business processes.
- Review mitigation responses developed by Divisions to address risks and confirm proposed remediation actions are feasible and appropriate.

7.4 Chief Information Security Officer will:

- Determine if a technology, system, program, or service requires a privacy impact assessment or other privacy compliance mechanism, such as a memorandum.
- Conduct privacy impact assessments for City Divisions.
- Provide Risk Treatment Plans to Divisions to identify privacy risks and outline measures to modify risk.
- Provide copies of PIA Reports to Division Heads upon request.
- Develop, maintain, and provide privacy impact assessment tools.
- Provide Risk Treatment Plan advice and interpretation guidance where appropriate.
- Maintain currency of the privacy impact assessment process based on industry best practices, and consult with partners, including the City Clerk, Chief Technology Officer, and the City's Health Information Custodians, when assessing possible changes to the privacy impact assessment process that will benefit the City.
- Engage and consult, as required, with the City Clerk, Chief Technology Officer, or City Solicitor, when developing guidance related to privacy impact assessments or risk treatment planning.

7.5 Chief Technology Officer will:

- Confirm that PIA Reports are completed as part of project review and gating processes for projects.
- Individually, or jointly with the City Clerk, Division Head or Project Sponsor, review PIA Report and documented risks prior to implementation of any technology, system, program, or service involving the collection or use of personal information or personal health information.
- Jointly with Division Heads, implement technology-based privacy requirements identified in Risk Treatment Plans.
- Jointly with the City Clerk, use their discretion to pause any technology, system, program, or service where privacy compliance issues have not been addressed in a manner that satisfies the privacy concerns raised in the Risk Treatment Plan or PIA Report.

7.6 Legal Services will:

- Review draft PIA Reports upon request.
- Provide guidance on compliance with applicable legislation and risk management options.

7.7 Division Heads will:

- Consult with the Office of the CISO as they determine if a privacy impact assessment is required.
- Ensure all information needed to complete the privacy impact assessment is submitted to the Office of the CISO
- Ensure adequate resources are budgeted in projects and other initiatives to cover the cost of any necessary privacy risk management activities.
- Consult with Office of the CISO, where necessary, to confirm adequate budget planning for privacy impact assessment expenses.
- Consult the City Clerk's Office and Office of the CISO to validate proposed privacy risk management actions.
- Sign off on the Risk Treatment Plan and accept privacy risks identified in Risk Treatment Plan on behalf of the Division.
- Request a copy of the PIA Report from the Office of the CISO, when necessary.
- Develop and implement Risk Management Plans.
- Consult with Legal Services regarding PIA Reports, Risk Treatment Plans, and Risk Management Plans.
- Provide a copy of a Risk Treatment Plan to the City Clerk's Office for review and confirmation prior to implementation of the Plan.
- Provide status of the Risk Treatment Plan's implementation to the City Clerk's Office and Office of the CISO.
- Ensure protection of personal information and personal health information collected, used, or disclosed by their Division or by contracted third parties and sub-contractors.
- Ensure all Project Sponsors in their Division adhere to these requirements for projects and initiatives.
- Document the implementation of each risk mitigation activity from a Risk Treatment Plan.
- Sustain risk mitigation activities as long as necessary to ensure privacy is protected.
- Ensure documentation of privacy risk mitigation is maintained to a standard of audit readiness.
- Communicate this policy to their staff and contract resources hired for projects.

7.8 Health Information Custodians will:

Under the Personal Health Information Protection Act (PHIPA), Health Information Custodians (HICs) are independent from the City and are accountable for appointing or designating a Head of Privacy—which may be the Head of their Division or the City Clerk–to accept privacy risks and comply with PHIPA on behalf of their organization. Where HICs engage or collaborate with the City on technology projects, they will:

- Determine if a technology, system, program, or service requires a privacy impact assessment or other privacy compliance mechanism, such as a memorandum.
- Ensure that a privacy impact assessment is completed for technologies, systems, programs, and services.
- Engage appropriate parties to complete privacy impact assessments, including the Office of the CISO or external assessors.
- Request the Office of the CISO share a copy of the PIA Report or Risk Treatment Plan with their Head of Privacy, as required.
- Accept privacy risks identified in the PIA Report and Risk Treatment Plan.
- Develop privacy risk mitigation options and controls based on the outcome/recommendations of the Risk Treatment Plan.
- Implement the Risk Treatment Plan.
- Ensure compliance with the PIA Report and Risk Treatment Plan.
- Share the PIA Report and Risk Treatment Plan with relevant stakeholders, including the City Clerk and the Office of the CISO.

8. Authority

The *Municipal Freedom of Information and Protection of Privacy Act (*MFIPPA) and R.R.O. 1990, Reg. 823 General requires institutions to take reasonable measures to prevent unauthorized access to records in their possession and to ensure that procedures are documented and put in place to safeguard personal information.

The *Personal Health Information Protection Act, 2004* (PHIPA), governs the collection, use, disclosure, and retention of personal health information by a health information custodian. City Health Information Custodians (HIC) are required to maintain high standards and safeguards to ensure the protection of personal health information. Any HIC that has not appointed a Head of Privacy or Chief Privacy Officer separate from the City Clerk must comply with this Policy.

The *City of Toronto Act*, *2006*, S. 200 governs the retention and preservation of records of the City and its local boards in a secure and accessible manner. S. 201, governs the retention and destruction of City records.

The Auditor General's report *Information Technology Projects Implementation: Information Privacy and Cybersecurity Review of Human Resource System*, dated February 3, 2021 recommends the following:

City Council request the Chief Technology Officer, enhance the management of cybersecurity and privacy risks as part of its IT project governance by:

- *Ensuring that cybersecurity and information privacy requirements and related budget are part of the acquisition, development, and design phases of technology projects. The Office of the Chief Information Security Officer and the*

City Clerk should be consulted to review the budget allocated for cybersecurity and information privacy for all City technology initiatives, transformations, and procurements.

- *Ensuring a process is in place to identify, analyze and communicate all cybersecurity and information privacy risks to all stakeholders at each project phase through a documented risk mitigation plan. The identified risks are either mitigated or formally accepted by the division head/project sponsor before the system is launched.*
- *Ensuring the remediation of open risks is completed within a specified timeline and are signed off by the division head/project sponsor before moving to next project development stage.*

9. References

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 (2005). Managing a Privacy Breach Guideline. Retrieved from: http://insideto.toronto.ca/clerks/policies/files/managing-privacy-breach.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, City Clerk's Office (2012). Responsible Record-Keeping Directive. Retrieved from: https://www.toronto.ca/wp-content/uploads/2017/08/9741-Responsible-Record-Keeping-Directive-Final_1.pdf

City of Toronto, City Clerk's Office (2011). Responsible Record-Keeping Guideline. Retrieved from: https://www.toronto.ca/wp-content/uploads/2017/08/9762-ResponsibleRecordKeepingGuidelinesFINAL.pdf

City of Toronto, Legal Services (2023). Municipal Code Chapter 169, Officials, City. Retrieved from: https://www.toronto.ca/legdocs/municode/1184_169.pdf

City of Toronto, Legal Services (2021). Municipal Code Chapter 217, Records, Corporate (City). Retrieved from: http://www.toronto.ca/legdocs/municode/1184_217.pdf

City of Toronto, Technology Services Division (2018). Acceptable Use Policy. Retrieved from: http://insideto.toronto.ca/itweb/policy/pdf/acceptable_use.pdf

City of Toronto, Technology Services Division (2022). Digital Infrastructure Strategic Framework. Retrieved from: https://www.toronto.ca/wp-content/uploads/2022/03/9728-DISFAcc2.pdf

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

10. Policy Approval

Provided by Kristie Pratt, Deputy City Clerk, Corporate Information Management Services, City Clerk's Office June 19, 2023.

11. Policy Review

The City Clerk's Office will review this Policy and its effectiveness as needed.

Appendices

Appendix A: Definitions

Personal health information (PHI) is identifying information about an individual in oral or recorded form, if the information is both:

1. in the custody or control of a City Staff member, who as a result, or in connection, of this Staff member performing their workplace responsibilities to the City in relation to any of the following tasks: (a) acting as a health care practitioner; a health service provider; placement co-ordinator; medical officer of health; or, (b) operating in whole or in part, a hospital; psychiatric facility; independent health facility/community health facility; community health/mental health centre, program, or service; long-term care home; care home; home for special care; retirement home; pharmacy; laboratory/specimen collection centre; or ambulance service; and;
2. the information: (a) relates to the individual's physical, or mental health; providing health care to the individual; health care payments; health care eligibility; eligibility for health care coverage; (including the identity of the individual's health care provider; the identity of the individual's substitute decision-maker; health history of the individual's family; and health number); or, (b) is a plan setting out the home and community care services a health service provider would provide to the individual.

Personal information (PI) 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*, section 2.

Privacy is a set of interests and rights that an individual has regarding his/her ability to control the collection, use, disclosure, and retention of his/her own personal information that is in the custody or control of a third party. Privacy is a limited, not an absolute right. Personal information may be collected from or about an individual, used, disclosed, or retained without their consent where specific legislation permits.

Privacy impact assessment (PIA) is a due diligence exercise to analyze the effects of a technology, system, program, or service design on the privacy of individuals.

Privacy Impact Assessment Form is a self-serve form, to be used by the business to complete the PIA request and submit it to the Office of the CISO for review. The form is used to create a separate document, a PIA Report, which is completed and reviewed by the Office of the CISO.

Privacy Impact Assessment Report is a report that identifies privacy risks and offer recommendations to address those risks.

Risk Management Plan is a document that describes the methodology and processes that will be adopted and used to carry out risk management activities. The document also identifies assumptions, roles and responsibilities, communications and whether risks will be mitigated or formally accepted by the Division Head / Project Sponsor.

Risk (Matrix) Log is a document that identifies, analyzes, and lists all risks in a project. The log should be continually revisited as new risks are discovered. The log outlines and describes risks, criteria, likelihood, impact, ranking, status, responsibility mitigation plan and contingency plan.

Risk Treatment Plan - a plan describing what risk mitigation options/ controls will be implemented. The Risk Treatment Plan should be comprehensive and provide all necessary information about the proposed actions, timelines, and resources. A risk treatment plan is designed to help ensure that risk treatment processes and controls are taking place.

Appendix B: Privacy Risk Treatment and Management Process

Divisions are accountable for ensuring their compliance with this Policy and maintaining a state of audit and investigation readiness. The City Clerk's Office, Office of the CISO, and Technology Services Divisions promote and enable compliance, but do not supervise the privacy related risk management and remediation activities outlined in the Risk Treatment Plan.

1. Identify

The Divisional contact or project manager completes and submits the PIA Form to the Office of the CISO. The PIA Form helps the Office of the CISO determine if a technology, system, program, or service will collect personal information, and if a formal privacy impact assessment is required. The PIA Form should be submitted during the design phase of a project or initiative to ensure there are adequate resources to identify, accept, treat, and manage privacy risks within the project or initiative's timelines.

2. Inform

The Office of the CISO prepares a PIA Report that identifies privacy risks in a technology, system, program, or service. The City Clerk and City Clerk's Office's Corporate Information Management Services (CIMS) unit, the Division Head, and the Chief Technology Officer are informed of privacy risks. PIA Reports are not shared with the Division Head by default. Division Heads may request a copy of the PIA Report from the Office of the CISO. The Digital Rights Protection team within the Office of the CISO maintains the authoritative copy of the PIA Report.

Risks from the PIA Report are transferred to the Risk Treatment Plan (RTP) by the Office of the CISO. The Risk Treatment Plan is provided to the appropriate risk owner for sign-off.

The PIA Report is shared, by default, with CIMS once the Risk Treatment Plan has been delivered to the Division Head.

The City Clerk will use their discretion to pause any projects that are not in compliance with this Policy.

3. Remediate

In consultation with the Office of the CISO, risk mitigation options and controls are outlined within the Risk Treatment Plan by the responsible Division. The Risk Treatment Plan, including mitigation responses, are signed-off by the Division Head and provided to the Office of the CISO.

Mitigation responses may be reviewed by the City Clerk's Office's Corporate Information Management Services unit prior to implementation to confirm that major risks have been identified and can be mitigated by the proposed actions.

The Division or Divisional project manager may centralize all project related risks and mitigation responses within a Risk Management Plan and Risk Log.

Technology Services Division may support implementation of risk mitigation responses within technologies, but Division Heads are responsible for ensuring the implementation satisfies the PIA Report and Risk Treatment Plan's recommendations.

4. Document
Divisions are responsible for documenting implementation of each risk mitigation activity from the Risk Treatment Plan within the Risk Treatment Plan itself or within a Risk Management Plan and Risk Log.

5. Evaluate
Divisions will conduct internal audits, program reviews and program evaluations to assess their compliance with this Policy.

Consequences of Non-Compliance
Failure to adhere to the PIA Policy may cause an unintentional release of personal information by City staff, resulting in a privacy breach. A privacy complaint can be filed internally with City Clerk's Office's Corporate Information Management Services business unit, or externally with the Information and Privacy Commissioner (IPC) of Ontario. When a complaint is received either internally or externally, a thorough investigation into the allegations is conducted.

In the event that CIMS receives an internal privacy complaint or experiences a privacy breach, CIMS staff will:

- Investigate the allegations/occurrence.
- Assess the program's compliance with privacy legislation.
- Review the Risk Management Plan, and Risk Management Plan and its implementation by the responsible Division.
- Make recommendations to bring the program into compliance.

CIMS will share its findings and recommendations to the Division Head and Office of the CISO.

Privacy complaints received and investigated by the IPC often result in a report being made public on its website, which may cause embarrassment to the City. If a privacy complaint is filed with the IPC, the Commissioner has the power to order the City to comply with their orders or recommendations. The order could include ordering the City to stop collecting personal information for the specific program under investigation, and ordering the program area to destroy the information that it has collected to date.

The Auditor General may be engaged to audit PIA Reports, Risk Treatment Plans, and Risk Management Plans in response to cybersecurity breaches or privacy breaches reported internally or externally.