Privacy Impact Assessment Policy

UNDER REVISION

Policy No. CIMS 004
Version No: 2.0
Approval Date: March 16, 2010
Revision Date: April 3, 2013

A Corporate Information Management Policy

Subject: Privacy Impact Assessment Policy

Policy No: CIMS 004
Version No: 2.0

Keywords: Privacy Impact Assessment, privacy, personal information, personal health information, security, PHI, PI, PII

Issued by: City Clerk's Office
Corporate Information Management Services

Issued on: April 3, 2013

Contact Information:

Director, Corporate Information Policy — Tel: (416) 397-0736

Corporate Information Management Services — 13W City Hall
100 Queen St. West,
Toronto, Ontario M5H 2N2

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
2.0	2020-09-11	City Clerk's Office	This policy is currently under revision.

Table of Contents

1. Introduction

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.

The City of Toronto is responsible for ensuring the protection 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. These principles identify the public expectation for access to the City's information and the protection of their privacy.

The City Clerk has authority under the Delegation of Duties and Responsibilities in the *Toronto Municipal Code*, to ensure safeguards are in place to protect personal information that is in the City's custody or control. It is the responsibility of all City staff to ensure these protections are in place within technologies, systems, programs or services.

Adverse consequences of not managing the City's information as a corporate asset include privacy breaches, identity theft, fraud, loss of trust by the public, and legal action, that may result in financial penalties imposed by the IPC and law suits filed against the City for breach of privacy.

2. Purpose

The purpose of this policy is to identify management's responsibilities relating to Privacy Impact Assessments (PIAs), and to reassure the public that the City builds privacy protective measures into its services, technologies, and/or systems.

3. Policy Statement

The City is committed to protecting the privacy of individuals when personal information is collected, used, disclosed or retained.

When planning a new project or making a substantial change in the way an existing program collects, uses, discloses or retains personal information, Divisions must contact the I&T Division, Risk Management and Information Security (RMIS)to determine the need for a PIA.

The City Clerk and Chief Information Officer will be notified of all new PIA projects prior to the actual assessment taking place.

Divisions will commit to working with I&T to complete a PIA prior to implementing new technology, system, program and/or service that involve personal information.

To contain costs, the PIA should be initiated at the beginning of the project. Retrofitting a system to reduce privacy risks after it is designed or implemented has proven to be expensive.

The City Clerk is authorized to put any City project on hold that contravenes the PIA Policy.

4. Policy Outcomes

(a) Divisions will provide the necessary resources (financial, technical and staff) to ensure that personal information is collected, used, retained and disclosed in compliance with applicable privacy legislation.

(b) A PIA is completed on all new services, technologies, and/or systems that involve personal information as identified under the screening process

(c) Completed PIAs are signed by the appropriate parties.

(d) A privacy and security risk management plan must be developed to address priority privacy and security risks. Priority risks must be resolved before implementing a technology system, program or service.

5. Application

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

This Policy does not apply to Elected Officials, Accountability Officers or City Agencies and corporations. The City of Toronto encourages City Agencies and Corporations to review, adopt or update this Policy appropriate to their business circumstances.

6. Requirements for PIA

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

1. New or increased collection of personal information, with or without the consent of individuals.
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, other government organizations or third parties. Electronic service delivery initiatives may involve shared service delivery models where data is shared with more than one program area.
4. New proposal may affect client privacy in the collection, use, disclosure and/or retention of personal information.
5. Proposal involving new technologies, for example, smart cards, wireless surveillance cameras, biometrics, etc. or reusing personal information that was collected for one purpose and using it for another purpose, e.g. police reference checks.

6. Submitting a Technology Acquisition Request Form (TARF) to purchase new software and/or hardware that may collect personal information (e.g. biometric fingerprint scanner/reader).
7. When collecting more information to verify the identity of an individual.
8. Data warehousing and/or data marts are being proposed.
9. Sharing City data with 3rd parties through contracting out or alternate service delivery models.
10. Significant changes to policies, business processes or systems are planned that may affect the physical or logical separation of personal information from other information within a system
11. Contemplating changes to security mechanisms used to manage and control access to personal information (e.g. granting citizens electronic access to their own information).
12. Existing programs and systems are being consolidated, re-engineered and/or involve changes in functionality (e.g. link 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/data or technology.

7. Roles and Responsibilities

City Manager will:

- ensure that there is compliance with the Privacy Impact Assessment Policy.

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.

City Clerk will:

Lead development, monitoring, implementation and compliance with this policy.

- authorize sign-off of the PIA report prior to implementation of any technology, system, program or service involving the collection or use of personal information or personal health information.
- liaise with the Chief Information Officer and responsible Division Head to resolve privacy and security concerns
- determines the standards and qualifications of the resources permitted to conduct a PIA

- review all PIA screening assessments for technology, system, program or services

- jointly with the Chief Information Officer, place a "hold" on technology, system, program or service where privacy compliance issues have not been addressed in a manner that satisfies privacy and/or security concerns raised in the PIA report.

Chief Information Officer will:

- authorize sign-off of the Privacy Impact Assessment report prior to implementation of any technology, system, program or service involving the collection or use of personal information or personal health information.
- liaise with the City Clerk and responsible Division Head to resolve privacy and security concerns raised during the course of the privacy assessment
- review all PIA screening assessments for technology, system, program or service
- jointly with the City Clerk, place a "hold" on technology, system, program or service where privacy compliance issues have not been addressed in a manner that satisfies privacy and/or security concerns raised in the PIA report.

Information and Technology Division will:

- determine if a project, service initiative or information system requires a PIA, or other privacy advice
- conduct PIAs and follow public sector PIA methodology to assess privacy risks
- consult and advise program staff about privacy risks and issues;
- I&T staff will determine if a PIA is required based on information provided about the project through the business case, project charter, etc.
- provide cost estimates including resource plans, time/effort estimates (i.e. Statement of Work);
- consult with staff of the City Clerk's Office and/or the Information and Privacy Commission about unique or high risk privacy issues;
- support City Divisions in complying with this policy and privacy legislation.

Division Heads will ensure:

- protection of personal information and personal health information collected, used or disclosed by their division or by contracted third parties and sub-contractors via appropriate privacy assessments
- that this policy is communicated to their staff
- that project managers (PMs) will contact Risk Management and Information Security (RMIS) of the I&T Division to determine if a PIA is

required and provide RMIS staff with detailed information about the project (e.g. business case, project charter)
- the members provide to RMIS additional documentation (e.g. forms, system requirements) and other relevant information relating to the technology, system, program or service
- adequate funding in the budget to cover the costs one or multiple PIAs
- authorize sign-off of the Privacy Impact Assessment report prior to implementation of any technology, system, program or service involving the collection or use of personal information or personal health information
- the development and implementation of a Risk Management Plan to resolve privacy, security and information risks
- that he/she signs the final PIA report.

Legal Services will:

- review draft PIAs upon request, with respect to legal issues identified in the report and will validate these issues with relevant orders from the Information and Privacy Commissioner.

8. Definitions

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.

Personal health information is defined under *PHIPA*, S. 4 and is information relating to the physical or mental condition of an identifiable individual. This includes, but is not limited to:
- the health history of one's family
- identification of an individual's health care provider
- payments of or eligibility for health care or health care benefits
- donation of body parts or of bodily substances for testing or examination
- health card number
- the identity of an individual's substitute decision maker.

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 (i.e. City of Toronto).

Privacy is not an absolute right in all situations. Personal information may be collected, used, disclosed or retained without the consent of individuals where specific legislation permits.

A **Privacy Impact Assessment Screening Tool** is a preliminary assessment of a project to determine if a PIA is required.

A **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.

A **Risk Management Plan** is a plan that identifies how the project sponsor will accept, avoid or reduce the risks identified for the project.

9. Monitoring and Compliance

Divisions will conduct internal audits, program reviews and program evaluations to assess their own degree of compliance with this policy.

The final PIA report will be provided to CIMS, City Clerk's Office; Internal Audit; and Information and Technology for information.

In the event that the City receives a privacy complaint or experiences a privacy breach, CIMS staff will investigate the allegations/occurrence, assess the program's compliance against privacy legislation and may make recommendations to bring the program into 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 CIMS 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.

Privacy complaints/breaches received internally by CIMS usually result in a mediated solution between the program area and the complainant. CIMS will send its findings and recommendations to the program manager, director and copy the division head.

Privacy complaints received by the IPC often result in their report being made public on their Web site 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 recommendations. The order could include ordering the City to stop collecting personal information and ordering the program area to destroy the information that it has collected to date.

10. 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 Ito

prevent unauthorized access to records in its 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. Any division of the City considered to be a health information custodian, (for example, Toronto Public Health) is required to maintain high standards and safeguards to ensure the protection of personal health information.

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.

Report No. 1, Clause 9(a) of the Audit Committee was adopted by Council at its meeting held on May 21, 22, and 23, 2003. The Auditor General's report included the following recommendation:

"12. The Chief Administrative Officer, in consultation with other City Commissioners, ensure that the implementation of new information systems are not initiated until Privacy Assessment Impact evaluations are completed. The requirement for a Privacy Impact Assessment be mandatory in all business cases supporting systems development where personal information is involved."

In addition, the Financial Planning Division's Capital Budget Policy, *Budgeting for IT Projects* #FS-FP-006, dated August 6, 2006 requires the following:

"All Programs submitting IT business cases supporting new systems development must commit to the completion of a Privacy Impact Assessment (PIA) as part of their business case submission, including associated costs as part of the implementation costs. New information systems that store personal data are not to be implemented until these PIAs are completed."

11. Applicable Policies and Resources

- Municipal Code Chapter 217
  http://www.toronto.ca/legdocs/municode/1184_217.pdf
- Acceptable Use Policy
  (http://www1.toronto.ca/City%20Of%20Toronto/City%20Clerks/Corporate%20Information%20Management%20Services/Files/acceptable_use.pdf)
- Information Management Accountability Policy
  http://wi.toronto.ca/intra/clerks/cco_policies.nsf/9A23FE79BA48081F85257A9900498FC5/$file/IMAP%20Version%201.pdf
- Responsible Record-Keeping Directive
  http://wi.toronto.ca/intra/clerks/cco_policies.nsf/FCB753C4FCBC50F3852579D500553288/$file/responsible_record_keeping_directive.pdf
- Responsible Record-Keeping Guideline

http://wi.toronto.ca/intra/clerks/cco_policies.nsf/74F900B01AE72B36852579D50055D858/$file/responsible_record_keeping_guideline.pdf

12. Approved by:

Joseph P. Pennachetti
City Manager
Version 1.0, March 16, 2010
Version 2.0, April 3, 2013

13. Policy Approval and Review

This policy will be reviewed every year or sooner if necessary. The revised policy will be approved according to the current process.