



CORPORATION OF THE TOWNSHIP OF ALBERTON

BY-LAW NO. 50/26

A By-law to adopt a Privacy Impact Assessment Policy for the Township of Alberton.

WHEREAS Section 11(2) of the *Municipal Act, 2001, S.O. 2001 c25, as amended*, provides that a municipality may provide any service or thing that the municipality considers necessary or desirable for the public, subject to the rules set out in subsection (4), and may pass by-laws respecting the following matters:

1. Governance structure of the municipality and its local boards.
2. Accountability and transparency of the municipality and its operations and of its local boards and their operations.
3. Financial management of the municipality and its local boards.
4. Public assets of the municipality acquired for the purpose of exercising its authority under this or any other Act.
5. Economic, social and environmental well-being of the municipality, including respecting climate change.
6. Health, safety and well-being of persons.
7. Services and things that the municipality is authorized to provide under subsection (1).
8. Protection of persons and property, including consumer protection.

AND WHEREAS Effective January 1, 2027, the *Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, Chapter M.56*, provides that a municipality shall implement policy, procedures and risk mitigation measures to protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information;

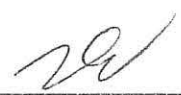
AND WHEREAS Privacy Impact Assessments (PIAs) are a requirement for municipalities effective January 1, 2027, and are a practical, strategic necessity for municipalities and must be completed before implementing any new program, system, or major upgrade to an existing system, to identify risks, confirm legal authority, and protect public trust;

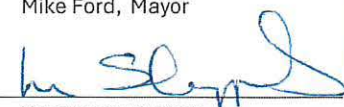
AND WHEREAS the Township of Alberton deems it expedient to implement a *Privacy Impact Assessment Policy* which sets out procedures and reporting mechanisms to be followed by the Township with regard to the collection, use, disclosure, retention and safeguarding of information before a new system, upgrade to an existing system or program is launched, in accordance with Section 28 of the *Municipal Freedom of Information and Protection of Privacy Act*;

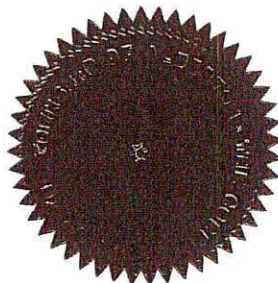
NOW THEREFORE the Council of the Corporation of the Township of Alberton enacts as follows:

1. **THAT** the *Privacy Impact Assessment Policy* attached hereto as Schedule "A" shall be and is hereby adopted.
2. **THAT** this By-Law shall come into force and take effect upon the final passing thereof.

READ A FIRST, SECOND AND THIRD TIME AND PASSED THIS 15th DAY OF OCTOBER, 2026.


Mike Ford, Mayor


Lisa Sheppard, Clerk





Privacy Impact Assessment (PIA) Policy

Corporate Administration Framework · Compliance with MFIPPA s. 28

Date of Council Approval: 15 October 2026

Effective Date: January 1, 2027

By-Law #: 50 /26

Resolution 2026-146

Review Cycle: Every three (3) years

Primary Owner: Clerk's Department / FOI Coordinator

Applicable Laws: MFIPPA, Municipal Act 2001

1. Purpose

Ontario municipalities are navigating an era of rapidly evolving technical advancements and regulatory and legislative changes. Technology advancements, improvements and changes to service delivery, cloud platforms, and data-sharing partnerships are transforming how municipalities collect, use, and protect personal information (PI).

Privacy Impact Assessments (PIAs) are a requirement for municipalities effective January 1, 2027, and are a practical, strategic necessity for municipal leaders. For example, when council approves initiatives such as new election or voter management software, cloud-based service platforms or data-sharing agreements. A Privacy Impact Assessment must be completed before implementation to identify risks, confirm legal authority, and protect public trust. PIAs help organizations anticipate risks tied to the collection, use, disclosure, retention, and safeguarding of PI—before a system or program is launched.

This policy establishes a standardized governance framework for managing institutional privacy risks within the Corporation. In compliance with the updated provisions of Section 28 of the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), this policy mandates the systematic completion of Privacy Impact Assessments (PIAs) before launching any new program or system that handles personal information. This assessment policy is intended to help the Township evaluate how it stores and collects information, identify potential risks and find solutions to mitigate risk. This policy will be updated from time to time to align with Information and Privacy Commissioner of Ontario's Guidelines, incorporating recommended best practices, and to ensure compliance with FIPPA and MFIPPA.

2. Scope

This policy applies to all municipal initiatives, departments, boards, committees and programs that collect, use, process, store, retain, or disclose Personal Information (PI) or Personal Health Information (PHI).

- **Inclusions:** Applies to all permanent, temporary, and contract staff, as well as third-party vendors, cloud-software software-as-a-service (SaaS) environments, and contracted service operators acting on behalf of the municipality.
- **Administrative Systems:** Explicitly encompasses routine municipal software infrastructures, including property tax billing systems, and building permit applications.

3. Privacy Principles

- a) **Accountability** – the Clerk shall be the individual responsible for personal information handling practices.
- b) **Limiting Collection** – collect only the personal information that is directly necessary to meet a program's objective.
- c) **Direct collection and purpose identification** – collect personal information directly from the individual and

- inform them of the purpose/reason for collection.
- d) Retention – only keep personal information for as long as necessary. (Note: Privacy Act regulations cite at least two (2) years following the last administrative use).
 - e) Accuracy – the Township must take reasonable steps to ensure the accuracy of the personal information.
 - f) Disposal – the Township must securely dispose of personal information in accordance with its Record Retention Policy requirements.
 - g) Limiting use – the disclosure of personal information should be limited, and in line with the original purpose of collection or a consistent use, or otherwise with the consent of the individual.
 - h) Safeguards – the Township will take steps to protect personal information from inappropriate access, use or disclosure.
 - i) Openness – the Township will be open and clear about how personal information will be handled (e.g. publish public notices regarding privacy).
 - j) Access – individuals have a right to request access to their personal information, and correct it, when necessary. Individuals will self-identify any changes or corrections necessary to administrative personnel who will update records promptly and accordingly.

4. Mandatory Triggers for a PIA

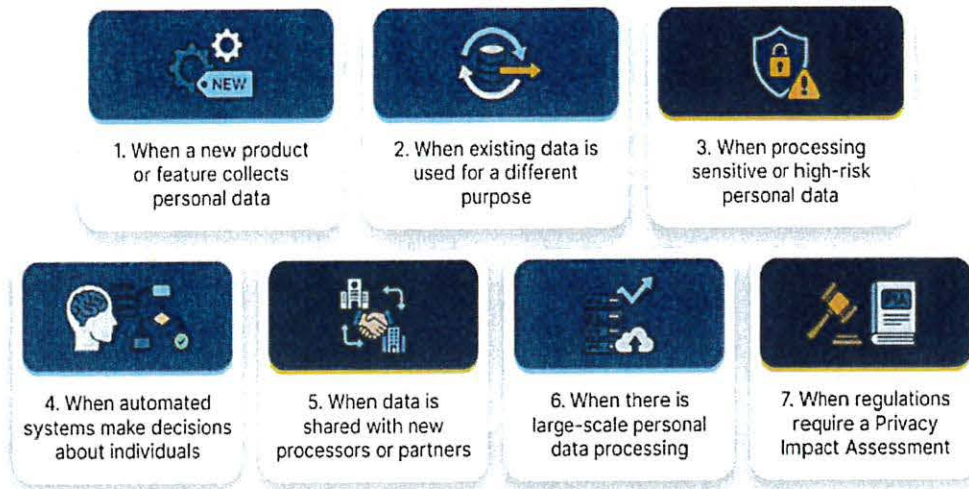
A written Privacy Impact Assessment must be initiated, finalized, and signed off **prior to** the operational rollout of any initiative meeting the following statutory criteria:

- **New Collections:** Launching any system, application, program, or operational channel that collects personal identifier data (e.g., names, billing addresses, financial metrics, phone numbers, IP configurations).
- **System Modifications:** Executing major upgrades, alterations, or business-process shifts affecting an active legacy system (e.g., transferring on-premise tax databases to cloud hosting platforms).
- **External Disclosures:** Instituting data-sharing agreements, third-party integrations, or Application Programming Interface (API) tunnels that expose municipal personal records to external commercial, provincial, or federal entities.
- **Surveillance Tech:** Deploying public-facing tech footprints, of which examples include: Closed-Circuit Television (CCTV) and automated license plate scanners.

5. Roles and Responsibilities

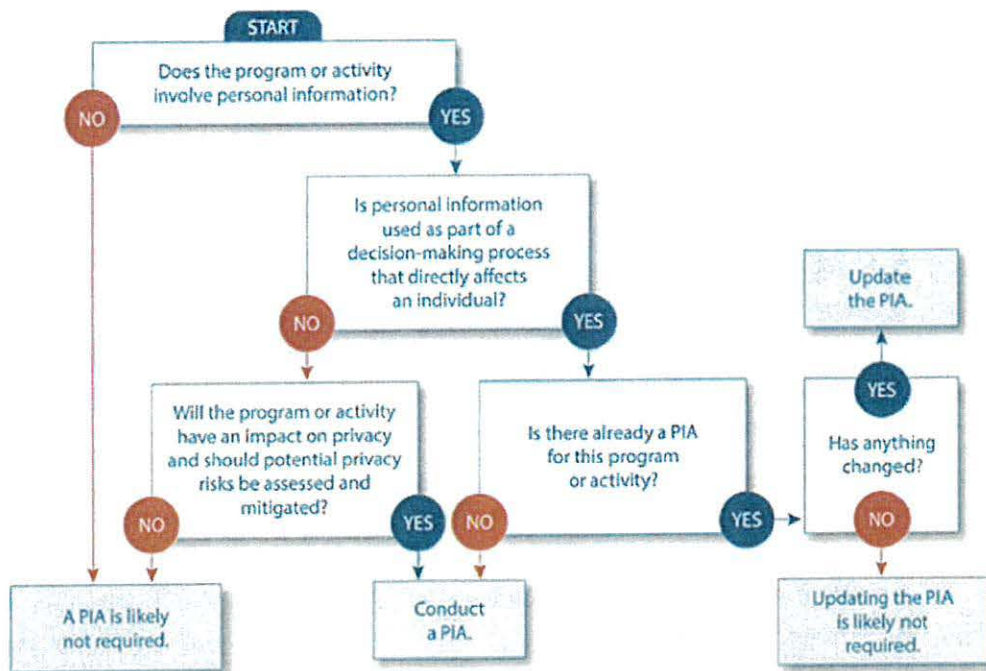
Role / Stakeholder	Core Privacy Accountability
Department Head / Project Lead	Initiates the PIA intake form; designs workflows using privacy-by-design concepts; and implements required technical or physical security controls.
Clerk/ FOI Coordinator	Serves as the primary advisory body; reviews data flows; cross-references statutory authority; maintains the central repository of corporate PIAs.
Information Technology (IT)	Validates digital security safeguards; checks encryption configurations, access logs, network boundary isolation, and vendor cyber postures.
Chief Administrative Officer- CAO/Clerk-Treasurer	Holds ultimate executive accountability for institutional compliance; executes final structural approvals for high-residual-risk deployments.

When to Conduct Privacy Impact Assessments

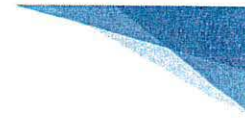


6. Operational PIA Procedure

All municipal departments must advance through the following structural workflow:



- **Step 1: Threshold Assessment:** Project lead completes an initial screening checklist. *If personal data touches the project, a full PIA is triggered.*
- **Step 2: Information Mapping:** The department charts detailed data inventory tracking the life-cycle of the data, specifically the collection, distribution, backup, and purge pathways.



- **Step 3: Statutory Analysis:** The Clerk verifies and checks appropriate legislative coverage (e.g., MFIPPA s. 28/29) and designs the mandatory public collection notices.
- **Step 4: Complexity Analysis:** Internal staff are generally well-placed to conduct a PIA. However, depending on the complexity of the project and availability of internal expertise, the CAO/Clerk-Treasurer may seek an external specialist to conduct the PIA. If the PIA is conducted by an external specialist, the PIA will be reviewed and approved by the CAO/Clerk-Treasurer who shall be responsible for implementing the recommendations of the PIA
- **Step 4: Risk Mitigation Matrix:** Threats (such as over-collection or vendor storage leaks) are listed alongside technical resolutions (like tokenization, zero-trust configurations).
- **Step 5: Review & Integration:** IT Security audits access logs and vendor SSAE-18 SOC 2 compliance. The Clerk outlines modifications for contractual templates.
- **Step 6: Official Execution:** The CAO/Clerk-Treasurer and Department Head sign off on the assessment report.
- **Step 7: Continuous Audit:** Systems undergo a formal re-review every 36 months, or immediately upon code modifications, vendor updates, or regulatory revisions.

**Municipalities are required to provide the Information and Privacy Commissioner of Ontario with PIA's upon request.*

7. Non-Compliance and Enforcement

Failure to execute a mandatory PIA before launching an operational workflow represents a serious regulatory breach. Non-compliance compromises municipal legal protections and would result in statutory intervention from the Information and Privacy Commissioner of Ontario (IPC).

- **System Halts:** The CAO/Clerk-Treasurer holds executive authorization to demand an immediate operational halt to any unassessed, new, or upgrade to existing processes that collect, use, store or retains personal information or personal health information.
- **Disciplinary Metrics:** Intentionally evading, bypassing, or ignoring mandatory assessment paths will trigger disciplinary investigation and actions up to and including employment termination.

8. Steps to be taken

Outlined below are the steps to be taken to prevent or reduce the likelihood of theft, loss or unauthorized use or disclosure of personal information and to mitigate risks to individuals in the event of such a privacy breach.

- **Administrative Safeguards:** The CAO/Clerk-Treasurer holds executive authorization and responsibility to conduct mandatory Privacy Impact Assessments (PIA's) on all new software and data-sharing programs and will document the risks and establish the legal authority before collecting data.
- **Technical Safeguards - Data Minimization:** Intentionally collecting, recording or storing only personal information that is absolutely necessary to fulfill the specific service.
- **Technical Safeguards – Data Permissions:** Enforce strict role-based access permissions so that staff can only view information essential to their immediate job duties.
- **Physical Safeguards –** Retention of physical files will be in secure, locked cabinets with access

restricted to authorized personnel.

- **Monitor Continuously** – conduct regular reviews, continuously review and update PIA's as changes occur in service.
- **Stay Informed** – regularly check for reports and recommendations and legislative changes to ensure compliance and best practices are implemented.

9. Mitigation steps to be taken

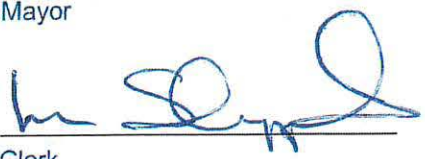
Outlined below are the steps to be taken to mitigate harm during a privacy breach. If a breach does occur, the Township shall act immediately to limit exposure and protect individuals from harm. The steps below are sourced from the practical guidance and clear mitigation framework of the office of the Information and Privacy Commissioner of Ontario and shall be adhered to.



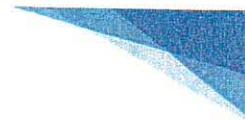
- **Containment:** Isolate the breach immediately by retrieving any hard copies, notifying IT security, resetting compromised passwords, changing electronic identification numbers and/or temporarily disabling affected networks.
- **Real Risk of Significant Harm (RROSH) Evaluation:** Assess the incident against the RROSH threshold. Analyze the data sensitivity (examples health information, financial numbers, or Social Insurance numbers) alongside the probability of malicious misuse.
- **Mandatory reporting and notification:** For breaches that reach the RROSH threshold, notify affected individuals and report the incident to the Information and Privacy Commissioner of Ontario as soon as feasible. Ensure the notifications detail the breach circumstances, state the specific data exposed, outline the Township's containment efforts, and direct the individuals to file an IPC complaint if they choose.
- **Provide actionable advice for victims** – Provide affected individuals with clear, immediate steps to protect themselves, such as placing fraud alerts on credit files, changing personal account passwords or monitoring specific banking transactions.
- **Remediation and review** – document the containment timeline completely, investigate the root-cause and patch system vulnerability to ensure the event will not be repeated in the future.



 Mayor



 Clerk



Schedule A – PIA Report Template

The Township of Alberton will utilize this PIA report template as a best practice document, as provided in the Privacy Commissioner of Ontario's Guide for Ontario's Public Institutions, but not as a substitute for legislation. When conducting a PIA and completing the report; always refer to legislation and updated guidelines to ensure compliance with FIPPA or MFIPPA.

Introduction

PIA Project Report Title	Department	Date	Individual who completed this PIA report

Objective

- What is the objective of this project?
- What is the purpose of the PIA Report? And are there any attachments/appendices?
- What is the response being sought and response timeline?

Executive Summary

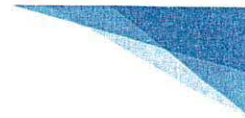
- Provide decision-makers with an overview of the project
- Summarize your key findings, recommendations and action items
- Note any outstanding privacy impact



General

Provide high-level context for your analysis and findings including but not limited to:

- Briefly describe the PIA process including the purposes and outcomes of the preliminary analysis, project analysis and privacy analysis and attach any completed questionnaires, checklists and supporting documents.
- Scope – briefly describe what is in-scope and out of scope in your PIA. Note any related projects, programs or systems, relevant PIA work or other risk analysis undertaken by other parties.
- Be sure to explain any specialized terms and acronyms used in your PIA analysis and documentation.



Project

Provide a summary and description of the project including as much detail as necessary that will allow reviewers and decision-makers to understand the project and information in your privacy analysis.

Accountability for the Project	Any related initiatives and linkages	Project partners and interested parties

Privacy

Describe the purpose(s) for which personal information is intended to be collected, used and disclosed, as applicable, and an explanation of why personal information is necessary to achieve the purpose.

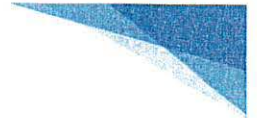


Identify the legal authority for the project and for collecting, using and disclosing personal information (eg. Privacy legislation such as FIPPA or MFIPPA) and be sure to include any references to related agreements with partners, agents and other third parties if applicable.

--

Details, Roles and Responsibilities

What type of information is intended to be collected, used and disclosed (as applicable)?	
Why is the collection of personal information necessary to achieve the purpose of the project?	
What is the source of personal information to be collected?	
Identify the legal authority for the project (eg. The applicable privacy legislation FIPPA or MFIPPA)?	
Identify the individuals and parties (internal & external to the Township) responsible for protecting privacy and briefly explain their role.	
Who will have access to the personal information (include all officers, employees, consultants or agents of the Township)	



Identify any limitations or restrictions imposed on the collection, use or disclosure of personal information.	
Retention period – what is the period of time that the personal information would be retained by the Township?	
Safeguards – explain all administrative, technical and physical safeguards, practices and measures that would be used to protect personal information from theft, loss or unauthorized use or disclosure.	
Risks to individuals – identify and summarize any risks to individuals in the event of a theft, loss or unauthorized use or disclosure of the personal information.	
Explain the change(s) to existing processes	
Who will be responsible for the privacy of personal information throughout its lifecycle?	

Information Flow

How will personal information be collected?	
How will personal information be used?	

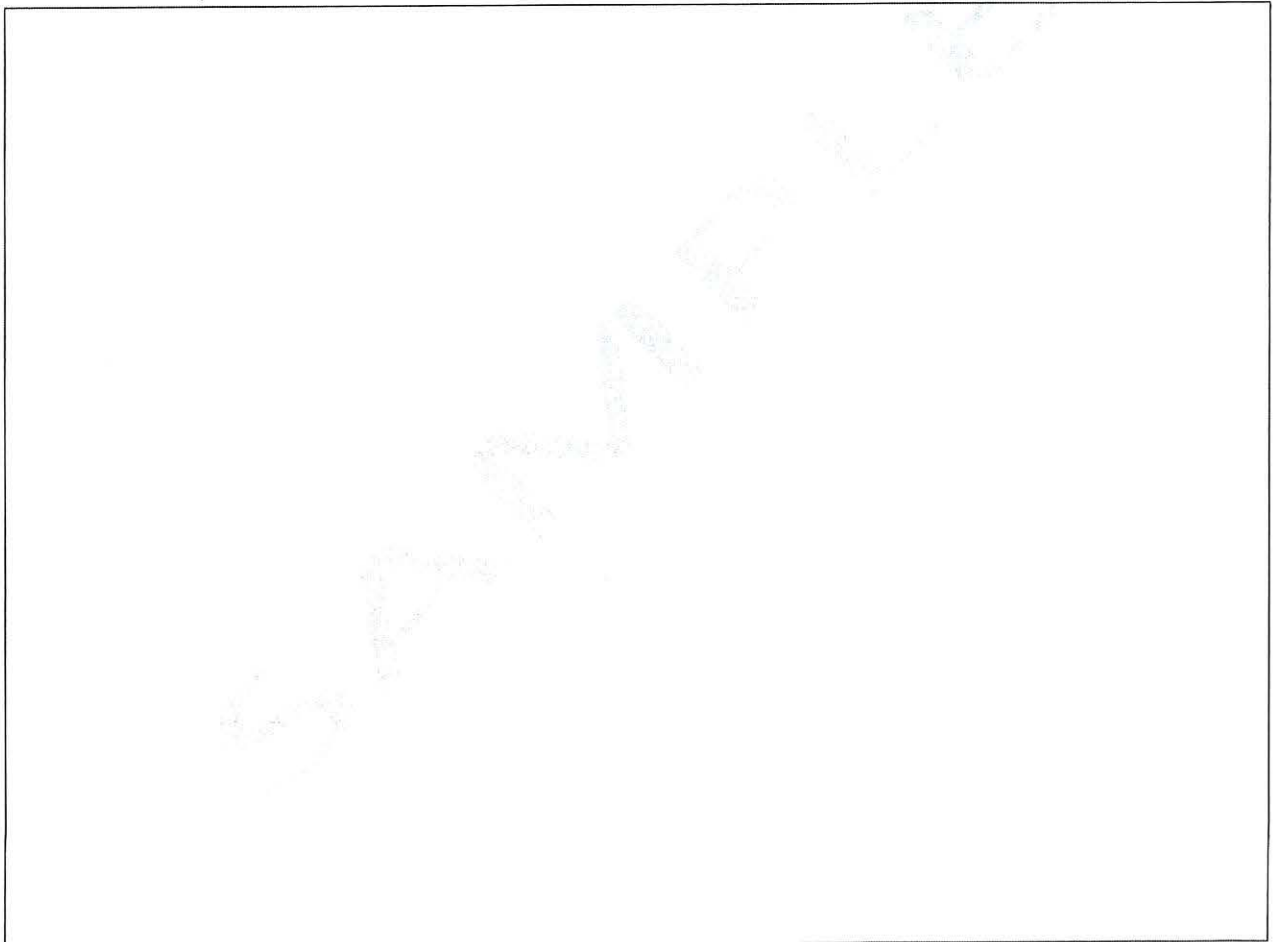


How will personal information be disclosed?	
How will personal information be secured?	
How will personal information be disposed of?	

Privacy Analysis

Explain the results of your completed privacy analysis and include the following:

- Your findings
- The privacy impact and risk(s) related to each finding
- Your recommendations on what needs to be done to protect privacy and comply with FIPPA or MFIPPA
- Your risk prevention and mitigation steps to (a) prevent or reduce the likelihood of a theft, loss or unauthorized use or disclosure of personal information from occurring and (b) mitigate the risks to individuals in the event of such an occurrence
- Identify the priorities and proposed timelines and who will be responsible for project implementation

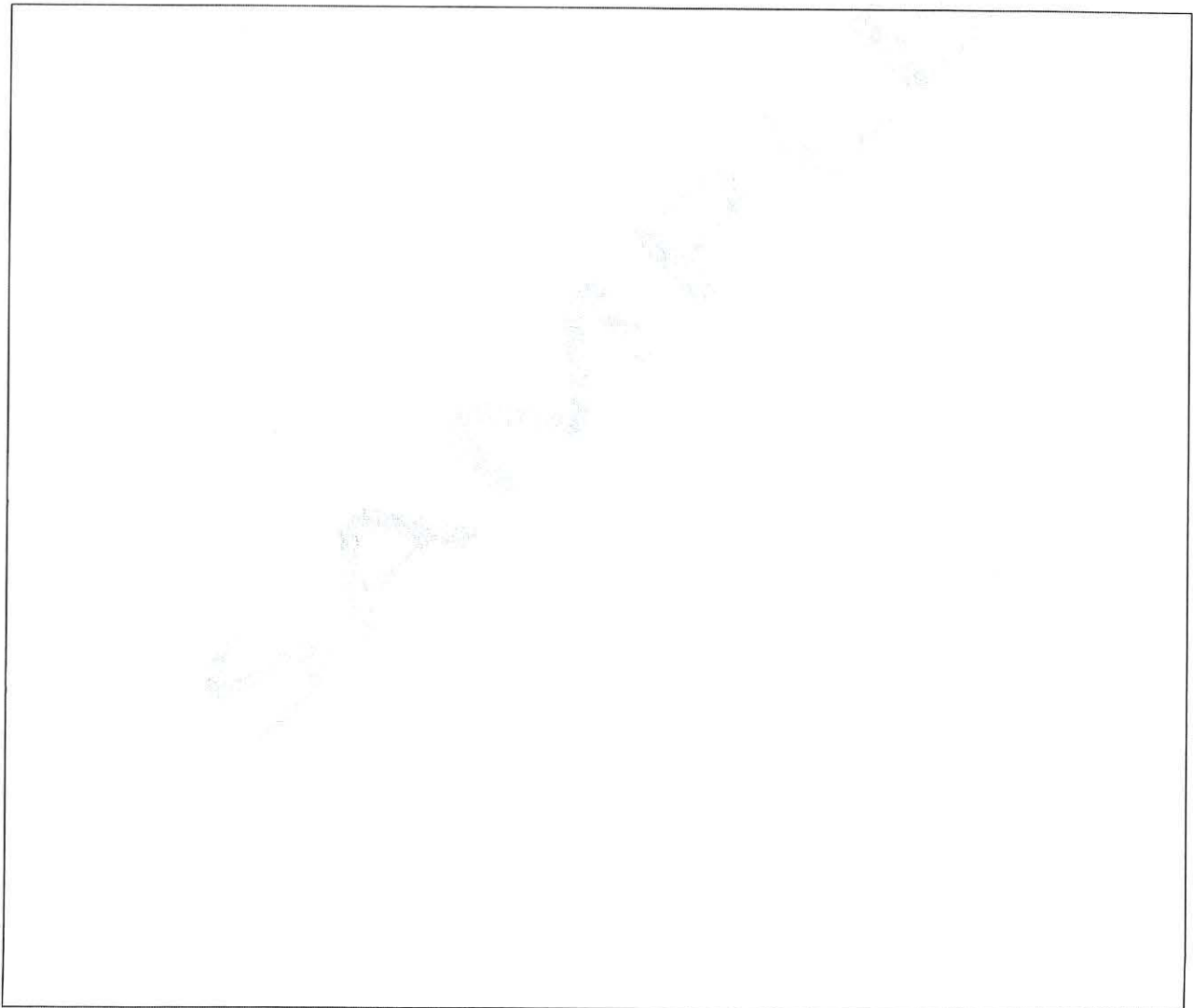


Conclusion



Include any final remarks relevant to your PIA, including but not limited to:

- Was your analysis successfully achieved or is there outstanding and further privacy work necessary that must be completed?
- Will this project enhance privacy protection and compliance with privacy requirements?
- Could this project be designed to avoid, eliminate or reduce some or all of the identified privacy risks?
- Could this project result in an unjustified invasion of privacy?
- Will this project involve new technology, business rules or processes for which the privacy risks are not known or well-documented?
- Highlight any required follow-up and next steps to your privacy analysis (eg. Timing and priorities for implementation of risk prevention, or requirements to update the PIA report in the future)
- Document where the Township will maintain the final approved PIA report and ensure that the location is known and accessible within the Township. PIA reports should be easily retrieved for review, updating and providing to the Information Privacy Commissioner (IPC) for Ontario.
- Make sure to include and attach any relevant documentation to support the findings and recommendations in this report.





Submitted by

The individual preparing the PIA shall sign below and acknowledge in writing, that they have prepared the findings and recommendations, understand the risk prevention and mitigation steps/action items, or acceptance of the privacy risks for the project.

Project Lead (Individual responsible for the preparation of this report)

By affixing my signature above, I acknowledge that I understand the findings, recommendations of the risk prevention and mitigation steps/action items, or acceptance of the privacy risks.

Note: Final approval requires the signing authorities authorized to bind the Corporation of the Township of Alberton to sign and acknowledge below.

Approval

The signing authorities authorized to bind the Corporation of the Township of Alberton shall sign below and acknowledge in writing, that they understand the findings and recommendations, and authorize implementation of the risk prevention and mitigation steps/action items, or acceptance of the privacy risks.

Mayor

By affixing my signature above, I acknowledge that I understand the findings, recommendations of the risk prevention and mitigation steps/action items, or acceptance of the privacy risks and authorize implementation.

CAO/Clerk-Treasurer

By affixing my signature above, I acknowledge that I understand the findings, recommendations of the risk prevention and mitigation steps/action items, or acceptance of the privacy risks and authorize implementation.