Privacy Management Plan & Administrative Directive

REFERENCE:	**ADOPTED BY:**
Access to Information Act, SA 2024, Chapter A-1.4 *Protection of Privacy Act*, SA 2024, Chapter P-28.5, *Protection of Privacy (Ministerial) Regulation* AR 143/2025 and *Protection of Privacy Regulation*, AR 132/2025 **Review Cycle:** Annually, or earlier where required **Classification:** Public version, with confidential technical/security appendices maintained internally	Director of Strategic, Administrative & Financial Services (Head of the Public Body for ATIA & POPA as per Bylaw 26-06 – Designated Officer Bylaw
PREPARED BY: Strategic, Administrative & Financial Services	**DATE:** June 11, 2026

TITLE: PROTECTION OF PRIVACY

POLICY STATEMENT:

1.0 PURPOSE

1.1. The purpose of this Privacy Management Plan and Administrative Directive (the "Plan") is to establish a comprehensive, practical, and accountable framework for how the Town of Strathmore collects, uses, discloses, accesses, corrects, protects, retains, disposes of, and manages personal information, data derived from personal information, and non-personal data in accordance with applicable laws. This Plan is intended to:

a) set out the roles, responsibilities, and general principles that the Town of Strathmore (the "Town") must follow to ensure compliance with the *Access to Information Act* ("ATIA"), SA 2024, Chapter A-1.4, the *Protection of Privacy Act* ("POPA"), SA 2024, Chapter P-28.5, *Protection of Privacy (Ministerial) Regulation* ("Ministerial Regulation"), AR 143/2025, and any other legislation referenced in the Plan;

b) demonstrate the Town's commitment to responsible privacy governance;

c) establish clear roles, responsibilities, and accountabilities for privacy and access compliance;

d) require Privacy Impact Assessments where new or changed programs, technologies, systems, practices, or services involve personal information or privacy risk;

e) ensure privacy incidents are reported, contained, assessed, documented, and remediated promptly;

f) provide guidance for third-party service provider arrangements involving personal information;

g) establish minimum requirements for training, safeguards, monitoring, auditing, and continuous improvement;

h) promote public trust, transparency, accountability, and lawful municipal service delivery.

i) foster public trust and confidence in the Town through openness and transparency regarding the collection and management of personal information;

j) ensure the Town takes reasonable security safeguard measures to protect and manage personal information in its custody or under its control against such risks of unauthorized access, collection, use, disclosure, or destruction;

k) ensure accountability within the Town in making reasonable efforts to provide access to personal information and records;

l) communicate expectations for employee conduct as outlined in the Town's policies and Administrative Directives; and,

m) set out a Privacy Incident Response Protocol to manage suspected or actual privacy incidents.

2.0 SCOPE AND APPLICATION

2.1. This Plan applies to all Town departments, business units, programs, services, systems, records, and activities involving:

a) personal information in the custody or under the control of the Town;

b) data derived from personal information;

c) non-personal data created, used, disclosed, retained, or managed by the Town;

d) access to information requests under ATIA;

e) correction requests under POPA;

f) privacy complaints;

g) privacy incidents and breaches;

h) privacy impact assessments;

i) third-party service providers that collect, use, disclose, store, transmit, retain, dispose of, or otherwise manage personal information on behalf of the Town; and

j) any municipal program, project, technology, administrative practice, or service involving privacy or information access considerations.

2.2. Where another Town policy, bylaw, agreement, or procedure imposes a higher standard of privacy, confidentiality, security, records management, or access control, the higher standard shall apply unless otherwise directed by law.

3.0 LEGISLATIVE AND POLICY AUTHORITY

3.1. This Plan is established under the authority of:

a) the *Protection of Privacy Act*;

b) the *Protection of Privacy Regulation*;

c) the *Protection of Privacy (Ministerial) Regulation*;

d) the *Access to Information Act*;

e) the *Access to Information Regulation*;

f) the *Municipal Government Act*;

g) the Town's Records Management Bylaw, retention schedule, policies, directives, and procedures;

h) the Town's policies relating to information technology, cybersecurity, procurement, contract management, and human resources; and

i) any other applicable enactment, bylaw, policy, standard, or legal obligation.

3.2. This Plan is intended to be interpreted in a manner consistent with applicable legislation. If there is a conflict between this Plan and an applicable statute or regulation, the statute or regulation prevails.

4.0 DEFINITIONS

4.1. The following definitions set out in the Administrative Directive have the corresponding meanings:

a) **Access to Information Request** means an application under ATIA for access to records for general or personal information in the custody or under the control of the Town including access to an individual's own personal information;

b) **Administrative Safeguards** means policies, procedures, training, confidentiality obligations, access approval processes, monitoring, and other administrative measures designed to protect information;

c) **AI System** means a technological system that uses automated processing, machine learning, generative AI, predictive analytics, algorithms, or similar tools to generate content, analysis, recommendations, decisions, predictions, classifications, or outputs;

d) **Confidential Information** means information that is not publicly available and that must be protected because of legal, operational, commercial, security, privacy, or public interest considerations;

e) **Control** means the Town has the authority over the creation, use, distribution, retention or disposition of the records;

f) **Correction Request** means a request by an individual to correct that individual's personal information in the custody or under the control of the Town;

g) **Custody** means records that are in the Town's possession and may include records supplied by a third party;

h) **Data Derived from Personal Information** means data created from personal information through data matching, analysis, transformation, aggregation, or other processes, where the resulting data remains connected to or derived from personal information as contemplated by POPA;

i) **Disposition** means the formal process of removing records from the Town's custody when the retention period is met, be deletion or destruction, transfer to archival holdings, or transfer to another organization;

j) **Employee** means Town staff and any other person who performs a service for the Town as an appointee, volunteer, or student, or under a contract or agency relationship with The Town as per section 1(h) of POPA;

k) **Head of the Public Body** means the person designated as the head of the Town for the purposes of ATIA and POPA, or where no designation exists, the person legally responsible for the administration and operation of the public body;

l) **Non-Personal Data** means information or data that does not identify an individual and is not reasonably capable of identifying an individual, including data created in accordance with applicable law from personal information or data derived from personal information.

m) **Personal Information** means recorded information about an identifiable individual including:

i. the individual's name, home or business address, home or business telephone number, home or business email address, or other contact information, except where the individual has provided the information on behalf of the individual's employer or principal in the individual's capacity as an employee or agent;

ii. the individual's race, national or ethnic origin, colour or religious or political beliefs or associations;

iii. the individual's age, gender identity, sex, sexual orientation, marital status or family status;

iv. an identifying number, symbol or other particular assigned to the individual;

v. the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics;

vi. information about the individual's health and health care history, including information about the individual's physical or mental health;

vii. information about the individual's educational, financial, employment, or criminal history, including criminal records where a pardon has been given;

viii. anyone else's opinions about the individual; and,

ix. the individual's personal views or opinions, except if they are about someone else.

n) **Personal Information Bank or "PIB"** means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. A PIB allows individuals to know the type of personal information the Town may have about them, how it is used, and the Town's authority for the collection;

o) **Privacy Complaint** means a concern or allegation raised by an individual who believes that the Town has collected, accessed, used, disclosed, retained, corrected, or otherwise handled personal information in a manner that is contrary to applicable legislation, policy, procedure, or reasonable privacy expectations.

p) **Privacy Incident** means a loss of, or unauthorized access to, use or disclosure of personal information;

q) **Privacy Impact Assessment or "PIA"** means a documented assessment and critical process used to help identify and address potential privacy with respect to new, or substantial change to an existing administrative practice, program, project or service that will involve the collection, use or disclosure of personal information;

r) **Privacy Officer** means an individual designated by the Head to oversee the Town's compliance with POPA, this Plan, and related privacy obligations;

s) **Public Body** means the Town of Strathmore as a local public body subject to ATIA and POPA;

t) **Service Provider** means an external organization, contractor, consultant, vendor, software provider, cloud provider, records storage provider, processor, or other third-party that performs services for or on behalf of the Town and may collect, use disclose, access store, transmit, retain, dispose of, or otherwise manage personal information;

u) **Record** means any electronic record or other record in any form in which information is contained or stored, including information in any written, graphic, electronic, digital, photographic, audio or other medium, but does not include any software or other mechanism used to store or produce the record.

5.0 APPLICABILITY

5.1. This Administrative Directive applies to:

a) All employees; and

b) All records containing personal information, regardless of format or location, that are in the custody or under the control of the Town.

5.2. This Administrative Directive does not apply to Elected officials.

6.0 GUIDING PRINCIPLES

6.1. The Town shall administer this Plan in accordance with the following principles:

a) **Accountability**: The Town is responsible for personal information in its custody or under its control, including information handled by service providers on its behalf.

b) **Authority**: Personal information shall only be collected, used, disclosed, retained, or disposed of where authorized by law and necessary for a lawful municipal purpose.

c) **Minimum Necessary**: Employees shall collect, access, use, disclose, and retain only the minimum amount of personal information necessary to perform authorized duties.

d) **Transparency**: Individuals should be able to understand why the Town collects personal information, how it is used, and how they may exercise access or correction rights.

e) **Security**: The Town shall use reasonable administrative, physical, and technical safeguards appropriate to the sensitivity, volume, format, location, and risk associated with the information.

f) **Accuracy**: The Town shall make reasonable efforts to ensure personal information used to make decisions affecting individuals is accurate, complete, and up to date.

g) **Privacy by Design**: Privacy risks shall be considered early in the development or procurement of programs, systems, services, technologies, and administrative practices.

h) **Access and Openness**: The Town shall support lawful access to records while protecting confidential information, personal privacy, solicitor-client privilege, security, and other interests protected by law.

i) **Proportionality**: Controls must be proportionate to the sensitivity and volume of information and the nature of the Town's operations.

j) **Continuous Improvement**: The Town shall review, assess, and update this Plan and related controls on an ongoing basis.

7.0 POLICY STATEMENT

7.1. Collection of Personal Information and Notice

a) The Town will only collect the personal information as authorized by law, for the purposes of law enforcement, or as is necessary for The Town's operating programs or activities.

b) Personal Information will only be collected directly from the individual the information is about, subject to exceptions under POPA.

c) When information is collected directly from an individual, notice is given to inform of the purpose, the legal authority for the collection, and the contact information of an individual who can answer questions about the collection, and The Town's intent, if any, to input the information into an automated system to generate content or make decisions, recommendations or predictions, subject to exceptions under POPA. Such notice will be given in a clear, conspicuous manner taking into account the manner in which the personal information is collected.

d) The Town is committed to providing a website that respects our visitor's privacy. Collection and management of personal information through the website is based on the legal authority and purpose expressed in the notice in accordance with POPA, and Policy on the website.

7.2. Use and Disclosure of Personal Information

a) The Town will maintain a directory of personal information banks (PIB's) and make it available to the public.

b) The Town may only use personal information to the extent permitted under ATIA and POPA.

c) The Town may only disclose personal information as permitted under ATIA and POPA.

d) Access to personal information will be granted in accordance with the privacy legislation and Town bylaws and policies.

7.3. Sale of Personal Information

a) The Town is prohibited from selling information in any circumstance or for any purpose, including for marketing or advertising purposes.

7.4. Accuracy and Correction of Personal Information

a) The Town will make reasonable efforts to ensure that personal information used to make a decision directly affecting an individual is complete and accurate.

b) Individuals shall have the right of access to records in the custody under the control of The Town containing their personal information, subject to limited and specific exceptions set out in ATIA.

c) In the event that an individual believes any of the personal information in the custody or under control of The Town is incorrect, incomplete, or otherwise

inaccurate, the individual to whom the personal information relates to may request that it be corrected.

d) Individuals requesting a correction of personal information, must provide as much detail as possible, including:

i. The specific records they want to correct.

ii. The department that they believe have the records needing to be corrected.

iii. The specific time period for the records they are requesting to be corrected.

7.5. Withdrawal of Consent

a) Where an individual withdraws their consent to the collection, use, or disclosure of their personal information, the Town shall promptly document such withdrawal and take all reasonable steps to ensure that any further collection, use, or disclosure of the individual's personal information is carried out in compliance with the withdrawal of consent, subject to any applicable legal or contractual obligations.

7.6. Retention and Disposition of Personal Information

a) Where The Town uses an individual's personal information to make a decision that directly affects the individual, The Town will retain the personal information for at least one year after using it.

b) The Town will retain and dispose of records containing personal information in accordance with The Town's Retention Policy and Records Management Policy.

7.7. Protection of Personal Information

a) The Town is committed to meeting its legal obligations to have reasonable security arrangements against such risks including unauthorized access, collection, use, disclosure, or destruction.

b) The Town protects personal information by implementing physical, technological, and/or administrative safeguards appropriate to the sensitivity of the information.

c) When an applicant makes an access to information request for their personal information, The Town will require them to provide acceptable proof to verify the applicant's identity, to show that they are the individual whose personal information is being requested.

d) All contracts entered into The Town that may involve that collection, use, or disclosure of personal information in the performance of the contract, will include a requirement for reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, or destruction.

7.8. Privacy Complaints

a) Individuals may make privacy complaints by contacting the Head of the public body.

b) The Town's Privacy Incident Response Protocol (Schedule B) will outline the process of how the Town receives and reviews complaints.

c) Investigation activities may include reviewing and assessing information provided, conducting interviews, and gathering evidence to document the events related to a suspected or actual privacy incident.

d) The Town will maintain a record of privacy complaints received across the organization in order to identify trends, recurring issues, process weaknesses, and opportunities for improvement.

7.9. Privacy Impact Assessment ("PIA")

a) The Town will prepare a PIA with respect to a new, or a substantial change to an existing, administrative practice, program, project or service that will involve the collection, use or disclosure of personal information, as prescribed in *POPA* and the *Ministerial Regulation.*

b) All PIAs will provide a level of detail commensurate with the complexity of the practice, program, project or service the PIA relates to.

c) A PIA must be submitted to the Office of the Information and Privacy Commissioner("OIPC") if one or more factors apply, as prescribed in *POPA* and the *Ministerial Regulation.*

7.10. Privacy Incident Response

a) The Town will investigate all privacy-related incidents, including actual and suspected incidents of privacy, and may respond to any privacy-related incident.

b) An investigation is triggered by the submission of a *Privacy Incident Report Form,* through the direction of the Office of the Information and Privacy Commissioner or the Access and Privacy Coordinator.

c) Investigation activities may include reviewing and assessing information provided, conducting interviews, and gathering evidence to document the events related to a suspected or actual privacy incident.

d) The Town's "Privacy Incident Response Protocol" (Schedule B) describes the roles and responsibilities for managing actual or suspected privacy incidents.

8.0 PRIVACY TRAINING

8.1. Mandatory Training

a) Pursuant to Section 6(1)(d) of the *Protection of Privacy Regulation*, the Town is required to provide training to all staff every two years. The training is mandatory for all employees and includes the obligation of employees under privacy legislation. All employees shall complete privacy and access training, during onboarding, periodically as required by the Town, when job duties materially change, after a privacy incident where remedial training is required, when legislative or policy changes require updated training.

8.2. Role-Specific Training

a) Additional role-specific training shall be provided to employees who regularly handle sensitive or high-volume personal information, including employees in Legislative Services, Human Resources, Finance, Taxation and Assessment, Utilities, Municipal Enforcement, Fire, Recreation, Family and Community Support Services, IT, Records Management, Legal & Risk Management, Communications, and any other high-risk function identified by the Privacy Officer.

8.3. Training Delivery Format and Curriculum

a) Training may be delivered either in person or through remote means, as determined by the Town in its sole discretion.

b) The Town may, in its sole discretion, implement, update, revise, or modify the content, format, and delivery of any mandatory privacy training from time to time to reflect operational requirements, evolving risks, and best practices, and to ensure that such training remains effective and responsive to the needs of employees. Mandatory privacy training will, at a minimum, introduce the basic concepts every employee needs to understand to help protect personal information and maintain public trust. The training explains what personal information is, why it matters, and how everyday actions can affect privacy and security. Employees will learn practical ways to recognize privacy risks, handle information responsibly, avoid common mistakes, and report concerns.

8.4. Training Records

a) The Town shall maintain training records documenting completion, date, module, employee name, and expiry or refresh requirements.

b) New hires will be required to complete and sign off on the Town's privacy training with in one month of commencing employment with the Town.

9.0 ROLES AND RESPONSIBILITIES

9.1. The Director of Strategic, Administrative & Financial Services is ultimately accountable for the Town's compliance with ATIA, POPA, and this Plan.

a) The CAO shall ensure that:

i. sufficient authority, resources, and support are provided to implement this Plan;

ii. departments cooperate with privacy and access requirements;

iii. significant privacy risks are escalated appropriately;

iv. the Town maintains appropriate policies, procedures, tools, and training; and

v. the Plan is periodically reviewed and updated.

9.2. Head of the Local Public Body is responsible for:

a) ensuring that the Privacy Officer is designated.

b) protecting personal information by making reasonable arrangements against such risks as unauthorized access, collection, use, disclosure or destruction as set out in section 10(1) of *POPA;*

c) all obligations of the Head of the Local Public Body under *ATIA* and *POPA* that relate to The Town;

d) maintaining an up-to-date delegation instrument for the Head of the Local Public Body's delegated powers and duties.

e) providing annual training to all employees of the Town.

f) communicating with the Office of the Information and Privacy Commissioner of Alberta, including coordinating any negotiations, mediations, inquiries, and investigations on behalf of The Town.

g) liaise with the Office of the Information and Privacy Commissioner, the Government of Alberta, legal counsel, insurers, and other authorities as appropriate.

9.3. The Privacy Officer is responsible for:

a) the day-to-day oversight of privacy compliance and implementation of this Plan.

b) The overall development, implementation, and management of access to information and protection of personal information withing the Town;

c) developing and implementing policies, guidelines, and procedures to manage the Town's compliance with *ATIA* and *POPA*;

d) assisting with establishing and endorsing standards and procedures to ensure compliance with the privacy protection measures in *POPA* regarding the collection, use disclosure, accuracy, retention, and safeguards of personal information;

e) leading The Town's training on *ATIA* and *POPA,* policies, procedures, and tools;

f) leading The Town's privacy incident response and Privacy Incident Response Team, when required.

g) The Privacy Officer shall:

i. develop and recommend updates to the Town's Privacy Management Plan and related procedures;

ii. advise departments on collection, use, disclosure, retention, and protection of personal information;

iii. oversee Privacy Impact Assessments;

iv. coordinate privacy incident response and breach notification processes, ensuring that the Head of the Public Body is informed in a timely manner;

v. facilitate correction requests;

vi. support the Head with privacy complaints;

vii. review privacy clauses in contracts, procurement documents, data sharing arrangements, and service provider agreements;

viii. support privacy training and awareness;

ix. maintain privacy-related registers, including PIA, incident, complaint, training, and service provider tracking records;

x. advise on AI, automated systems, data matching, surveillance, and non-personal data initiatives;

xi. report material privacy risks, trends, and compliance issues to senior leadership; and

xii. recommend corrective actions, policy updates, and control improvements.

9.4. Managers are responsible for:

a) Ensuring all employees are compliant with the *Protection of Privacy Administration Directive.*

9.5. Human Resources is responsible for:

a) Assisting the Head of the Local Public Body with onboarding and training requirements for staff.

b) Assisting the coordination of annual training through Citation Canada.

c) ensuring each new hire has received and understands the Privacy Management Program.

d) Ensuring all employees receive access and privacy training as applicable to their role.

9.6. Employees are responsible for:

a) Participating in access and privacy training to understand appropriate collection, use, protection, management, disclosure, correction, and disposition of personal information as required by their job duties and responsibilities;

b) Only collecting, using, and disclosing personal information as authorized by POPA;

c) Implementing reasonable safeguards to protect personal information;

d) Participating in PIAs to help identify and address potential privacy risks with respect to a new, or a substantial change to an existing, administrative practice, program, project or service that will involve the collection, use or disclosure of personal information;

e) Responding to access to information requests in a timely manner by searching for, documenting and producing all responsive records;

f) Reporting any Privacy Incidents to the Head of the Public Body, and limiting the scope of impact of any privacy incident when possible;

g) Reviewing privacy recommendations and implementing the recommended privacy risk mitigation strategies where possible;

h) Making factual corrections to personal information without a formal request under POPA, if this is practical and expedites public business, when directly requested by the individual whom the personal information relates to; and

i) Notifying their supervisor of any questions they may have about the Privacy Management Program.

j) Engaging the Head so that it can be determined whether legal advice is required regarding the collection, use, or disclosure of personal information for new programs and services

k) All employees shall:

i. collect, access, use, and disclose personal information only as authorized;

ii. protect information from unauthorized access, use, disclosure, loss, destruction, or alteration;

iii. use Town-approved systems and tools for Town business;

iv. report suspected privacy incidents immediately;

v. complete mandatory privacy training;

vi. comply with confidentiality obligations;

vii. cooperate with access requests, correction requests, privacy complaints, PIAs, and investigations; and

viii. seek guidance where uncertain.

10.0 CONTRACTORS AND VOLUNTEERS

10.1. All contractors and volunteers shall:

a) collect, access, use, and disclose personal information only as authorized;

b) protect information from unauthorized access, use, disclosure, loss, destruction, or alteration;

c) use Town-approved systems and tools for Town business;

d) report suspected privacy incidents immediately;

e) complete mandatory privacy training;

f) comply with confidentiality obligations;

g) cooperate with access requests, correction requests, privacy complaints, PIAs, and investigations; and

h) seek guidance where uncertain.

11.0 MANDATORY PRIVACY POLICIES AND PROCEDURES INCORPORATED INTO THIS PLAN

11.1. The following policies and procedures form part of the Town's Privacy Management Plan. They may be maintained within this Plan, as appendices, or as separate supporting policies, standards, procedures, forms, or tools approved by the Town:

a) Privacy Officer designation and governance procedure;

b) Collection, use, disclosure, access, and sharing of personal information standard;

c) Access to Information request procedure;

d) Correction request procedure;

e) Privacy Impact Assessment procedure;

f) Privacy incident and breach response procedure;

g) Privacy complaint procedure;

h) Security classification standard;

i) Administrative, physical, and technical safeguards standard;

j) Records retention, secure disposal, and litigation hold procedure;

k) Service provider privacy and procurement procedure;

l) Consent management procedure;

m) AI, automated systems, and emerging technology procedure;

n) Data matching and data derived from personal information procedure;

o) Non-personal data creation, use, disclosure, and management procedure;

p) Surveillance, CCTV, and monitoring procedure;

q) Employee privacy training and awareness procedure;

r) Public access to PMP procedure;

s) Ongoing assessment, audit, and review procedure; and

t) Privacy register and documentation procedure.

12.0 AI, AUTOMATED SYSTEMS, AND EMERGING TECHNOLOGY

12.1. AI and Automated Systems shall be used in accordance with the Town's AI Policy attached as Schedule "E".

13.0 CONSEQUENCES OF NON-COMPLIANCE

13.1. Employees who fail to adhere to the Administrative Directive and any associated standards and procedures may be subject to corrective action, including dismissal from employment, or the specified terms outlined in their employee contract. Failure to comply with the duties imposed by *ATIA* or *POPA* or otherwise acting in contravention of the legislation may lead to penalties or offences under *ATIA* and/or *POPA*.

14.0 ATTACHMENTS:

Schedule A – Delegation Order
Schedule B – Privacy Incident Response Protocol
Schedule C – Privacy Complaints Response Protocol
Schedule D – Correction to Personal Information Protocol
Schedule E – AI Policy
Schedule F – Surveillance Policy
Schedule G – Records Management Bylaw
Schedule H – Records Management Policy
Schedule I – Retention Schedule
Schedule J – PIA Template Completion Guide
Schedule K – Personal Information Bank
Schedule L – Non-Personal Information Policy
Schedule M – Security Classification System

APPENDICIES:

Appendix I – Access to Information Form
Appendix II – PIA Template
Appendix III – POPA Privacy Forms Package
Appendix IV – OIPC Privacy Breach Notification Form

Director of Strategic, Administrative & Financial Services

June 11, 2026

Schedule "A"

DELEGATION ORDER

Duty, power or function of Head	**Section reference**	**Retained by Head – Director of SAFS**	**Delegated to Privacy Officer (aka Manager of Communications, Marketing & Legislative Services)**	**Delegated to other person(s)** (provide title(s) – specific or generic)
Collection, Correction, Protection of Personal Information				
Authority to set aside collection requirements	5(3), (4)	X		
Authority to decide on requests for correction of personal information	7(1)		X	
Duty to correct, annotate or link personal information, duty to notify previous recipients	7(3), (4)		X	
Duty to give notice to individual requesting correction	7(7)		X	
Authority to transfer a request for correction	8		X	
Duty to ensure protection of personal information by making reasonable security arrangements	10(1) Regulation (MIN) 2, 3		X	X (Legal Counsel and Manager, Information Technology)
Duty to notify the affected individual when there exists a significant risk of harm	10(2) Regulation (MIN) 4		X	
Duty to ensure protection of data derived from personal information	20		X	
Duty to ensure protection of data derived from non-personal data	24		X	
Use and Disclosure of Personal Information				
Establishing rules for electronic consent	Regulation 2(4)(a)	X		
Establishing rules for oral consent	Regulation 2(5)(a)	X		
Authority to disclose to guardian of a minor	54(1)(e)		X	

Duty, power or function of Head	**Section reference**	**Retained by Head – Director of SAFS**	**Delegated to Privacy Officer (aka Manager of Communications, Marketing & Legislative Services)**	**Delegated to other person(s)** (provide title(s) – specific or generic)
Authority to disclose to relative or adult interdependent partner of deceased individual	13(1)(s)		X	
Authority to disclose to avert imminent danger to health or safety	13(1)(cc) Regulation 1(1)(b)		X	
Authority to approve conditions for disclosure for research and statistical purposes and for administration of research agreements	15		X	
Reviews and Complaints				
Authority to ask the Commissioner for advice	28(1)	X	X	
Authority to require Commissioner to examine original record on site	29(4)	X		
Right to make representations to the Commissioner	41(6), (8)	X		
Duty to comply with Commissioner's Order	44	X	X	
General Provisions				
Duty to publish a directory of the body's personal information banks and keep it current	57(2), (5)		X	
Duty to record uses or disclosures of personal information not included in directory	57(4)		X	

Delegation Table – Administrative Responsibilities in the *Protection of Privacy Act* and Regulation that May be Assigned

Duty, power or function of public body	Section reference	Retained by Head	Delegated to Privacy Service Manager	Delegated to other person(s) (provide title(s) – specific or generic)
Collection, Accuracy and Retention of Personal Information				
Establishing controls over the collection, use and disclosure of personal information	2(a)	X		
Authorizing routine correction of personal information	2(b)		X	
Ensuring authorized purpose of collection	4		X	
Assuring proper collection and notification	5		X	
Assuring accuracy of personal information	6(a)		X	
Applying retention standards	6(b)		X	
Use and Disclosure of Personal Information				
Assuring appropriate uses	12		X	
Assuring appropriate purposes of data matching	17		X	
Assuring appropriate uses of data derived from personal information	18		X	
Assuring appropriate purposes of disclosure of data derived from personal information	19	X	X	
Assuring appropriate purposes for creation of non-personal data	21 Regulation (MIN) 5(1)		X	
Assuring appropriate use and disclosure of non-personal data	22, 23 Regulation (MIN) 5(2)		X	

Schedule "B"

PRIVACY INCIDENT RESPONSE PROTOCOL

PURPOSE

This Privacy Incident Response Protocol ("Protocol") outlines the steps that must be followed by all Employees when a suspected or actual breach of privacy occurs. The Protocol allows the Town to identify, manage and respond to privacy incidents. The purpose of this Protocol is to:

a) Identify roles and responsibilities in responding to a privacy incident; and

b) Establish steps to be followed when responding to a privacy incident.

WHAT IS A PRIVACY INCIDENT?

A privacy incident means a loss of, or unauthorized access to, use or disclosure of personal information. The Town's definition of privacy incident is aligned with that of the Office of the Information and Privacy Commissioner ("OIPC") of Alberta. This would include any event that results in personal information in the custody or under the control of The Town being collected, accessed, used, copied, modified, disclosed, or disposed of in an unauthorized manner, either deliberately or inadvertently.

KEY STEPS IN RESPONDING TO PRIVACY INCIDENTS

Initiate steps 1 through 3 as soon as a suspected or actual privacy incident has been identified. The Privacy Officer is accountable for all privacy incident activities.

1. Report

1.1. A suspected or actual privacy incident should immediately be reported by any employee to the Privacy Officer.

1.1.1. Employees can report a privacy incident using the internal Privacy Incident Report Form (Internal) available in M-Files and the Staff Portal.

1.1.2. The public can fill out a Privacy Incident Report Form (External) available on the Town's website.

1.2. The Privacy Officer will notify the Head of the Public Body, including the Chief Administrative Officer of a suspected or actual privacy incidents. The Head will coordinate for the Town's insurance provider to be notified.

2. Contain

2.1. Identify the scope of the privacy incident and contain it.

2.2. The Privacy Officer, with the affected department(s) will take and document immediate steps to contain the privacy incident and to secure the related records or information systems to prevent any further privacy incident from occurring. Information Technology may be engaged to assist with containment. Examples of containment activities include:

2.2.2. Stopping the unauthorized practice;

2.2.3. Recovering records;

2.2.4. Shutting down the information system(s) that may have been breached;

2.2.5. Revoking or changing computer access codes or correcting weaknesses in physical security; and

2.2.6. Calling an unintended recipient to request written confirmation of the destruction of a document received in error.

2.3. Employees should be mindful not to destroy any evidence that may be valuable in determining the cause and extent of the privacy incident, or that will allow the Town to take appropriate corrective action. This information is also required to be retained for insurance purposes.

2.4. The Privacy Officer will notify the RCMP if the privacy incident involves theft or other criminal activity.

3. Investigate and Evaluate

3.1. Once the privacy incident is contained:

3.1.1. The Head of the Public Body and/or the Privacy Officer will assign resources to investigate with the involvement of other parties, as necessary, and complete the following:

3.1.1.1. Identify and analyze the events that led to the privacy incident;

3.1.1.2. Obtain all relevant evidence;

3.1.1.3. Document the privacy incident and containment activities;

3.1.1.4. Inventory all personal information that was subject to the incident and determine the number of affected individuals;

3.1.1.5. Determine the real risk of significant harm; and,

3.1.1.6. Recommend a Privacy Incident Response Team, where required.

3.2. The Privacy Officer will lead an objective investigation and address any real or perceived conflicts of interest. The Privacy Officer will determine and involve appropriate individuals and/or third-party investigative services, as required.

3.3. All privacy incident investigations will result in a *Letter of Findings*.

4. Notify Affected Individuals

4.1. The Privacy Officer will determine whether notification is required to be given to the affected individual(s), the OIPC and the Minister. In making the determination, the Access and Privacy Coordinator will consult and collaborate with the affected department(s).

4.2. Notification to affected individuals(s) is based on whether the privacy incident creates a risk of significant harm to an individual. Prompt notification can help affected individual(s) mitigate the damage by taking steps to protect themselves.

4.2.1. "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, loss of business or professional opportunities, identity theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property, other legal harms, and financial losses.

4.2.2. When assessing whether a privacy incident creates a real risk of significant harm to an individual, the Privacy Officer must consider all relevant circumstances, including the following factors: (i) whether there is a reasonable basis to believe that the personal information has been misused or will be misused; (ii) whether the loss of, unauthorized access to, or unauthorized disclosure of personal information occurred as a result of malicious intent; (iii) the sensitivity of the personal information that was lost, accessed, or disclosed without authorization; (iv) the mitigating measures taken by the Town or any other factors that reduce the risk of significant harm; and (v) any other relevant factors.

4.2.3. The Privacy Officer will document the assessment of these factors as part of the privacy incident investigation. The assessment will be used to determine whether notification is required to the affected individual(s), the Commissioner, and the Minister, as applicable.

4.3. Notification to affected individual(s) occurs directly unless direct notification could cause more harm, is cost prohibitive or contact information is not available. In such instances, indirect notification may occur.

4.4. Affected department(s) Director(s) must assign a point of contact within three days of receiving the request from the Privacy Officer. The assigned point of contact will be identified as the Town's contact, to answer questions about the privacy incident, on the Letter of Notification to the affected individual(s).

4.5. If the affected department(s) director(s) are unable to agree to an assigned point of contact within two days of receiving the request, the Privacy Officer will inform the Head of the Local Public Body. The Head of the Local Public Body will contact the affected department Director(s) to obtain the point of contact.

4.6. Notifications to individuals should include the following information:

4.6.1. Date of the privacy incident and the date the incident was discovered;

4.6.2. Description of the privacy incident;

4.6.3. General description of information lost, accessed, used or disclosed without authorization;

4.6.4. Steps taken so far to mitigate the harm or risk of harm;

4.6.5. Steps the affected individual can take to further mitigate the risk of harm;

4.6.6. Contact information of an individual within the affected department who can answer questions or provide further information;

4.6.7. That individuals have a right to complain to the OIPC; and

4.6.8. Any other relevant information.

4.7. Where appropriate, Senior Leadership (including affected Director, Head of the Local Public Body, Human Resources representative, Department Manager, and Department Director) will be provided information related to privacy incidents in order to support:

4.7.1. The response activities;

4.7.2. The implementation of recommendations; and

4.7.3. Monitor and follow-up actions to prevent future privacy incidents.

Individual Informing	**Individual / Group to be Informed**	**When to Inform – Privacy Incidents**
Anyone aware of an incident.	Privacy Officer	All Incidents
Privacy Officer	Affected Department Director	Initial risk and harms assessment – This is based on information supplied in the *Privacy Incident Report Form.* • Incidents that *may* require notification to affected individuals; and, • Incidents that *may* impact the financial, legal or reputation of The Town. *<u>Post risk and harms assessment</u> – This is based on the evidence obtained through the investigation. • Incidents requiring notification to affected individual(s); and, • Incidents impacting the financial, legal or reputation of The Town. * *Will require assignment of point of contact in affected department to address questions from affected individual(s).*

	Head of the Local Public Body	Incidents requiring notification to affected individual(s); Incidents requiring notification to OIPC and the Minister; Incidents requiring notification to third-party service providers; and, Incidents impacting the financial, legal or reputation of The Town.
Privacy Officer	Head of the Public Body Senior Leadership Team	Incidents impacting the financial, legal or reputation of The Town.

5. Prevent

5.1. Once the immediate steps have been taken to mitigate the risks associated with the privacy incident and notification has been completed (if required) the Access and Privacy Coordinator and/or the Privacy Incident Response Team will develop prevention strategies to mitigate against similar future privacy incidents.

5.2. Mitigation and prevention strategies should reflect the significance of the privacy incident and whether it was a systemic or isolated event. Strategies may include a review of:

5.2.1. Physical safeguards (locks, alarms, security monitoring);

5.2.2. Technical safeguards (restricting access, encryption on portable devices); and

5.2.3. Administrative safeguards (policies, contractual clauses).

6. Follow-up

6.1. The Town tracks all privacy incidents across the organization and uses the information to identify trends in the types of privacy incidents occurring. This information can help identify underlying patterns with respect to personal information handling practices and may help prevent future privacy incidents.

6.2. Access to Information and Investigations section will follow-up with the affected department(s) on the implementation of recommendations.

7. Privacy Incident Response Team

7.1. Depending on the circumstances of the privacy incident, a Privacy Incident Response Team may be established by the Access and Privacy Coordinator to respond to a privacy incident. Activities may include carrying out containment and assisting with notification to affected individuals to minimize any current, ongoing, or future privacy risks.

7.2. Membership of the Privacy Incident Response Team is determined by the Access and Privacy Coordinator and varies depending on the context of the privacy incident. Where

appropriate, that affected department(s) may identify subject matter experts as resources to support the Privacy Incident Response Team.

7.3. The Privacy Incident Response Team may include representation from the following:

Team Member	Role
Privacy Officer	Leads all activities and decisions by the Privacy Incident Response Team, including escalation and notification decisions. Manages the privacy incident response activities to contain, investigate, evaluate, document and make recommendations to mitigate future privacy incidents.
Legal and Risk Management	Provides an assessment of the Town's legal position and legal advice pertaining to the privacy incident. This may include a review of legal, regulatory and contractual obligations. Reviews external communications to ensure that liability risk is managed.
Information Technology	Provides information systems and technology analysis related to the privacy incident. Leads the containment activities as it relates to information systems and technologies.
Human Resources	Provides personnel management and guidance related to the privacy incident.
Communications	Provides support in the development of a communications plan, with tactics, timelines, and key messages for the purpose of preserving the Town's reputation, and trust with employees and the public.
Affected Departments (Subject Matter Expert(s) (SME)	Provides accurate incident details related to the privacy incident. Ensures that the department perspective is considered.

7.4. The *Privacy Incident Response Procedure* will include step-by-step instructions to help the Privacy Incident Response Team carry out its responsibilities.

8. Roles and Responsibilities

Individuals	Roles	Responsibilities
All Employees	Employees need to be alert to the potential for personal information to be compromised, play a role in identifying, notifying, and containing a privacy incident.	• Report suspected or actual Privacy breaches to their department APPA and supervisor and/or Access and Privacy Coordinator;

		• Immediately undertake containment efforts; and • Assist with privacy incident investigations as required, including making factual corrections to privacy incident information
Privacy Officer	The Privacy Officer is accountable for the Town's response to a privacy incident by ensuring that all key steps of the *Privacy Incident Response Protocol* are implemented. The Privacy Officer must address escalation decisions in a timely manner, confirms notification requirements, and determines the need to assemble a Privacy Incident Response Team. Access to Information and Investigations manages the response activities to a privacy incident. Response to a privacy incident may include working collaboratively with affected department(s) to contain, investigate, evaluate, document and make recommendations to mitigate future privacy risks.	• Assemble and lead the Privacy Incident Response Team, when warranted; • Act as decision maker to involve third-party investigative services, as required; • Notify the Royal Canadian Mounted Police (RCMP) if the privacy incident involves theft or other criminal activity; • Inform the Head of the Local Public Body if escalation required for a point of contact for inclusion on the Letter of Notification to address questions from affected individual(s); • Make escalation decisions related to privacy incidents; • Issue a Letter of Findings; • Determine whether to provide notification upon review of incident; • Notify affected individual(s), as required; • Notify and work with the OIPC, as required; • Notify the Minister, as required; • Issue recommendations to mitigate privacy incidents and follow-up on implementation of

		recommendations with affected department(s); • Close privacy incident response and debrief the Privacy Incident Response Team; • Collect, monitor, and assess all privacy incidents and identify trends and opportunities to prevent future privacy incidents; • Conduct annual tabletop exercises with the Privacy Incident Response Team; and • Ensure Privacy Incident Response Team members are trained and in a state of readiness.
Department Subject Matter Expert (SME)	Department SMEs are individuals who are familiar with the privacy incident details. This individual supports the accuracy of incident documentation and the advancement of activities to close a privacy incident. The department SME plays a central role in triggering internal communications to the Town's Senior Leadership and Town Council.	• Review and fact-check Draft Letter of Findings; • Consult with the Department Director to assign a point of contact within 2 days of receiving a request from the Access and Privacy Coordinator. This person will address questions from affected individual(s); and • Inform department leadership on the facts relevant to the privacy incident.
Department Managers	Department Managers work collaboratively with Privacy Officer to execute the key steps to responding to a privacy incident. Affected department(s) have a role in mitigating recurring risks by implementing recommendations.	• Develop and implement a communication plan, as required; • Implement recommendations to mitigate privacy incidents; • Consult Human Resources on personnel management actions, as required; and • Inform and communicate with the Department Director, as required.

Directors	The Department Director plays a central role in ensuring the Town's Senior Leadership Team is aware of privacy incidents.	• Consult Human Resources on personnel management actions, as required; • Inform and communicate with the Department General Manager, as required; and • Assign a point of contact for inclusion on the Letter of Notification to address questions from affected individual(s).
Head of the Local Public Body	Foster public trust and confidence in The Town.	• Maintain overall accountability for The Town's Privacy Management Program; and • Inform the affected Department Director(s) if escalation is required to assign a point of contact for inclusion on the Letter of Notification to address questions from affected individual(s)
Privacy Incident Response Team	Supports timely response to more complex privacy incidents.	• Assess, scope, and contain privacy incident; • Mitigate privacy risks; • Resource for affected department(s); and • See table in Section 7, above for further details.

Schedule "C"

PRIVACY COMPLAINT RESPONSE PROTOCOL

PURPOSE

This Privacy Complaint Response Protocol ("Protocol") outlines the steps that must be followed by all Employees when a privacy complaint is received by The Town. The Protocol allows The Town to receive, assess, manage, investigate and respond to privacy complaints in a fair, timely and consistent manner.

The purpose of this Protocol is to:

a) identify roles and responsibilities for responding to privacy complaints; and

b) establish the steps to be followed when receiving, reviewing and resolving privacy complaints.

WHAT IS A PRIVACY COMPLAINT?

A privacy complaint is a concern or allegation raised by an individual who believes that the Town has collected, accessed, used, disclosed, retained, corrected, or otherwise handled personal information in a manner that is contrary to applicable legislation, policy, procedure, or reasonable privacy expectations.

A privacy complaint may relate to matters such as:

a) collection of personal information that the individual believes was unnecessary or unauthorized;

b) use of personal information for a purpose not permitted by law;

c) disclosure of personal information without authority;

d) unauthorized access to personal information;

e) failure to safeguard personal information appropriately;

f) concerns about retention, correction, or accuracy of personal information; or

g) dissatisfaction with how a previous privacy matter was handled internally.

A privacy complaint is distinct from a privacy incident. A privacy complaint is the concern raised by an individual; a privacy incident is the event or occurrence involving possible unauthorized access, use, disclosure, loss, or other compromise of personal information.

KEY STEPS IN RESPONDING TO PRIVACY INCIDENTS

A privacy complaint received by any employee must be promptly forwarded to the Head of the Public Body.

1.0 Receive and Report

1.1. Employees who receive a privacy complaint verbally, by email, in writing, or through another channel must document the complaint and forward it to the Head of the Public Body as soon as practicable.

1.2. Members of the public may submit a privacy complaint by contacting the Head of the Public Body.

1.3. The complaint should, where possible, include:

(a) the complainant's name and contact information;

(b) a clear description of the concern;

(c) the date or approximate date of the event(s);

(d) the department, program area, or service involved;

(e) any supporting records or evidence; and

(f) the outcome or resolution sought by the complainant.

1.4. If the complaint is received by a department directly, that department must preserve all relevant records and refrain from altering, deleting, or destroying information that may be relevant to the review.

2.0 Acknowledge and Assess

2.1. Upon receipt of the complaint, the Head of the Public Body will assess the complaint to determine its nature, scope, urgency, and appropriate process.

2.2. The Head of the Public Body will acknowledge receipt of the complaint and open a complaint file.

2.3. The Head of the Public Body will conduct a preliminary assessment to determine whether the matter is:

(a) a privacy complaint;

(b) a privacy incident requiring activation of the Privacy Incident Response Protocol;

(c) a request for access to information;

(d) a request for correction of personal information;

(e) a general service complaint; or

(f) another matter outside the scope of this Protocol.

2.4. If the complaint identifies a suspected or actual privacy incident, immediate containment and response measures may be initiated under the Privacy Incident Response Protocol while the complaint review continues.

2.5. If the complaint falls outside the scope of this Protocol, the complainant will be informed and, where appropriate, redirected to the appropriate department, process, or external body.

2.6. The Head of the Public Body will identify and address any real or perceived conflicts of interest. Where appropriate, another reviewer, department, or external resource may be assigned to support an objective review.

3.0 Investigate and Evaluate

3.1. Once the complaint has been assessed, the Head of the Public Body will lead or assign an objective review of the complaint.

3.2. The review may include:

(a) identifying the specific issue(s) raised by the complainant;

(b) gathering and reviewing relevant records;

(c) interviewing employees or other individuals with knowledge of the matter;

(d) identifying applicable legislation, policy, procedure, contractual terms, or operational practices;

(e) determining whether personal information was collected, used, disclosed, accessed, retained, corrected, or otherwise handled appropriately; and

(f) assessing whether immediate corrective action is required.

3.3. The Head of the Public Body may involve appropriate internal parties and subject matter experts, including Legal, Information Technology, Human Resources, Communications, or affected department representatives, as required.

3.4. Where relevant, the Head of the Public Body will determine whether the complaint reveals:

(a) a policy gap;

(b) a training issue;

(c) a process weakness;

(d) non-compliance with internal requirements;

(e) the need for corrective action; or

(f) the existence of a privacy incident not previously reported.

3.5. All privacy complaint investigations shall be documented in writing and conclude with a written summary of findings, conclusions, and any recommended corrective actions.

4.0 Respond

4.1. The Head of the Public Body will ensure that the complainant receives a response once the review is completed.

4.2. The response should be provided in writing, unless another format is appropriate in the circumstances.

4.3. The response should include, where appropriate:

(a) a summary of the complaint;

(b) the scope of the review conducted;

(c) the findings of the review;

(d) whether the complaint was substantiated, partially substantiated, or not substantiated;

(e) any corrective or mitigating steps taken or proposed;

(f) any further steps available to the complainant; and

(g) contact information for follow-up questions.

4.4. Where the complaint identifies a significant legal, operational, reputational, labour-relations, or public-interest issue, the Head of the Public Body will notify appropriate leadership in accordance with internal escalation practices.

4.5. If the complaint reveals that notification is required under the Privacy Incident Response Protocol or applicable law, that notification process will be managed separately and in coordination with the affected department(s).

5.0 Prevent

5.1. Where a complaint is substantiated in whole or in part, The Town will take reasonable steps to address the issue and reduce the likelihood of recurrence.

5.2. Remedial actions may include:

(a) correcting inaccurate information or records, where appropriate;

(b) changing administrative practices;

(c) strengthening physical, technical, or administrative safeguards;

(d) updating privacy notices, forms, or collection practices;

(e) clarifying roles and authorities;

(f) providing targeted coaching or training;

(g) reviewing contracts or service arrangements; and

(h) revising policies, procedures, or guidance materials.

5.3. Prevention measures should be proportionate to the significance of the issue and whether the matter reflects an isolated event or a systemic concern.

6.0 Follow-up

6.1. The Town will maintain a record of privacy complaints received across the organization in order to identify trends, recurring issues, process weaknesses, and opportunities for improvement.

6.2. The Access and Privacy Coordinator will follow up with the affected department(s), as required, to confirm implementation of recommendations or corrective actions.

6.3. Lessons learned from privacy complaints may be used to support staff training, policy review, risk assessments, and continuous improvement within The Town's Privacy Management Program.

Schedule "D"

CORRECTION OF PERSONAL INFORMATION PROTOCOL

PURPOSE

This procedure outlines the process for responding to requests to correct personal information in the custody or under the control of The Town.

1. Submitting a request for correction of personal information

1.1. An individual who believes their personal information is incorrect, incomplete, or inaccurate may submit a request for correction.

1.2. Requests for correction should:

(a) be submitted in writing;

(b) identify the record containing the personal information;

(c) describe the correction requested; and

(d) provide supporting documentation, where applicable.

1.3. Requests may be submitted to the Privacy Officer. Should a request be sent to another Town employee, the employee will forward the request to the Privacy Officer.

2. Review of Request

2.1. Upon receipt of the request, the Privacy Officer will review the request and consult with the affected department(s), as necessary.

2.2. The Town may request additional information or clarification from the applicant if required to properly assess the request.

2.3. The Privacy Officer may request the relevant department locate records.

2.4. The Town will determine whether:

(a) the information is personal information relating to the applicant;

(b) the information is inaccurate, incomplete, or outdated; and

(c) the requested correction is supported by evidence.

3. Decision and Timelines

3.1 If the correction request is accepted, Privacy Officer shall:

(a) correct the personal information where reasonable and appropriate; and

(b) notify any relevant department or third-party service provider, where appropriate and practicable. The corrected personal information will be used once approved.

3.2 If the correction request is refused in whole or in part, The Town will provide written reasons for the refusal.

3.3 The Privacy Officer will document the outcome of the correction request.

3.4 The Town will respond to correction requests within a reasonable timeframe and in accordance with applicable legislative requirements.

Schedule "E"

AI POLICY

Administrative Directive Policy on the use of AI in the Workplace

Strathmore

POLICY NUMBER: ####-AD

REFERENCE:	**ADOPTED BY:** CAO Insert Date
PREPARED BY: Legislative Services	**DATE:**

TITLE: Policy on the Use of AI in the Workplace

POLICY STATEMENT

1.0 PURPOSE

This policy governs the use of any generative AI Tool within the Town of Strathmore (the "**Town**"). The inappropriate use of AI can create significant risks to the Town, and any use of AI must be approved by the Town prior to its use, except as otherwise permitted for public or non-sensitive information in accordance with this policy.

2.0 SCOPE AND APPLICATION

2.1. This policy governs the use of AI in any form and manner by Users. The scope of this policy includes, but is not limited to, all internal applications and all third-party applications that leverage AI (e.g. ChatGPT and similar platforms). For greater certainty, "use" includes, without limitation, using AI to draft, summarize, revise, analyze, translate, generate, classify, or otherwise process content, data, code, images, audio, video, communications, records, or other materials. This policy also applies to Approved AI Tools and Unapproved AI Tools.

3.0 DEFINITIONS

3.1. The following definitions set out in the Administrative Directive have the corresponding meanings:

AI Output means any content, response, recommendation, summary, analysis, draft, calculation, code, image, or other result produced by an AI Tool.

AI Tool means any software, platform, application, or system that uses artificial intelligence, machine learning, generative AI, automation, predictive analytics, or similar technology.

Approved AI Tool means an AI Tool that has been reviewed and approved for Workplace Use in accordance with the Town's privacy, security, information technology, records management, legal, and procurement requirements and that is categorized as: (A) an "Enterprise AI Tool"; or (B) a "Public AI Tool".

Artificial Intelligence (AI) means technology or software that performs tasks commonly associated with human intelligence, including generating content, analyzing information, identifying patterns, making predictions, providing recommendations, or supporting decision-making.

Confidential Information means non-public information held by or belonging to the Town, including, but not limited to, contracts, Town financial or budget documents, procurement records, internal policies, business plans, legal or operational strategy, operational information, procurement documents, legal advice, privileged information, security information, third-party information received in confidence, and other non-public Town business records or other information not expressly approved for public release.

Enterprise AI Tool means an AI Tool that is licensed by the Town, accessed through an assigned and active Town-issued account, and managed within the Town's technology environment in accordance with the Town's security, privacy, information technology, records management, legal, procurement, training, monitoring, logging, audit, and governance controls.

Generative AI means AI that creates new content, including text, images, audio, video, code, summaries, reports, emails, presentations, or other materials in response to Prompts.

Highly Sensitive Personal Information means Personal Information requiring the strictest protections because of its sensitivity, vulnerability context, or risk of significant harm if lost, misused, accessed, or disclosed without authority, including, without limitation, biometric information about an individual, financial information about an individual, and personal information respecting a minor, senior, or vulnerable individual .

Human Oversight means meaningful review, judgment, and accountability by an authorized person before relying on, approving, publishing, submitting, or acting on AI-generated output.

Non-personal data means data, including data derived from personal information, that has been generated, modified, anonymized, or aggregated so that it does not identify any individual, and cannot reasonably be used to identify or re-identify any individual.

Personal Information means recorded information about an identifiable individual, including name, contact information, identification numbers, employment information, financial information, health information, images, opinions, correspondence, or any other information that identifies or could reasonably identify an individual.

Prohibited AI Use means any use of AI that is not permitted under this Policy, including use that involves Confidential Information, Personal Information, or Highly Sensitive

Personal Information in unapproved tools or violates applicable laws, policies, or contractual obligations.

Prompt means any input provided to an AI Tool to generate a response or output, including questions, instructions, data, documents, images, or other content.

Public AI Tool means an AI system that is publicly available, not licensed as an enterprise service for the Town, and not managed or controlled within the Town's technology environment, whether or not accessed through a personal account.

Public Information means information that has been expressly approved for public release by the Town, or information that is publicly available from external sources and contains no Confidential Information, Personal Information, or Highly Sensitive Personal Information.

Unapproved AI Tool means any AI Tool that is not expressly designated as an Approved AI Tool.

User means any employee, contractor, consultant, volunteer, elected official, student, or other person authorized by the Town to use AI Tools and/or Town technology, systems, information.

Workplace Use means the use of AI for any task, communication, document, decision, analysis, project, service, or activity connected to the Town's work, operations, or responsibilities.

4.0 INTENDED OUTCOMES

4.1. Data Classification

All information must be evaluated and classified prior to use with AI Tools. The classification level determines which AI Tools, if any, may be used. Where there is any uncertainty regarding classification, the information must not be used in AI Tools unless appropriately authorized.

The following classifications apply;

4.1.1 Public Information may be used in both approved Enterprise AI Tools (e.g., Microsoft Copilot) and Public AI Tools (e.g., ChatGPT, Claude, Gemini, Perplexity) for purposes such as research, drafting, and summarization. All AI Outputs must be reviewed for accuracy and must not misrepresent Town information.

4.1.2. Confidential Information and Personal Information may only be used in approved Enterprise AI Tools and only where all applicable conditions are met, including that the tool is approved, the use case is authorized, the user is properly licensed, and appropriate safeguards are in place such as access controls, audit logging, and data residency compliance. Confidential Information must not be used in Public AI Tools or Unapproved AI Tools under any circumstances. Where permitted, use

must follow data minimization and anonymization practices, and all AI Outputs must be subject to Human Oversight.

4.1.3. Personal Information and Highly Sensitive Personal Information is prohibited from use in all AI Tools, including approved Enterprise AI systems, except where explicitly authorized by the Town following formal review, risk assessment, and implementation of enhanced safeguards. In most cases, Highly Sensitive Personal Information must not be entered into any AI Tool and must only be handled within approved secure systems.

4.1.5 In all cases, Users are responsible for ensuring compliance with this Policy. AI Tools must not be used as the sole basis for decisions affecting residents, employees, financial outcomes, legal matters, or operations. Where there is any conflict between data classification requirements and permitted AI Tool usage, the more restrictive requirement applies.

4.2. **Review and Approval of AI**

Prior to using any AI, Users must ensure that the AI has been reviewed and approved in writing by the Town in accordance with this policy. The review process will assess the security controls, compliance standards, transparency, allocation of liability, privacy and data protection measures, and the data retention and deletion capabilities of the proposed AI. Without limiting the foregoing, the Town may consider whether the proposed AI: (a) stores Prompts or AI Outputs; (b) uses Prompts, AI Outputs, or usage data for model training or service improvement; (c) permits administrative controls over retention, deletion, access, and audit logging; and (d) is appropriate for the intended use case and category of information. Schedule "A" sets out any Approved AI Tools that may be used by Users in accordance with this policy. Schedule "A" may also identify approved users, approved use cases, approved categories of information, and any conditions or restrictions applicable to the use of a particular AI Tool.

4.3. **Access to AI**

Use of Enterprise AI Tools will be granted to authorized Users on a need-to-know basis. Each User shall utilize a personalized username and password in accordance with the Town's standards (*i.e.*, complexity, etc.). Users who use Enterprise AI Tools are responsible for ensuring that they log out of such technology when not in use and must take all necessary precautions to prevent unauthorized access.

All employees are granted permission to utilize Approved AI Tools and must complete training provided by the Town on the risks and responsible use of AI and compliance with this policy prior to such use. Employees must also complete any additional or updated training required by the Town from time to time, including where there are material changes to Approved AI Tools, applicable law, Town practices, or this policy. Users must sign a declaration, acknowledging that they have read, understood, and agreed to comply with this policy, including any approval conditions, restrictions, and requirements applicable to their use of AI. Users must not use Public AI Tools to process Confidential Information, Personal Information, or Highly Sensitive Personal information.

4.4. **Quality Assurance and Ethical Considerations**

4.4.1. Users are responsible for ensuring that their use of AI and any content generated or produced using AI aligns with the Town's values, ethics, and quality standards. AI Outputs must not be used if it breaches the rights of others or is misleading, false, harmful, offensive, or discriminatory. All AI Output must be reviewed by an appropriate human decision-maker before it is relied upon, shared, published, or otherwise used by the Town. Users remain responsible and accountable for verifying the accuracy, completeness, appropriateness, and legal compliance of any AI Output.

4.4.2. Where AI use is permitted, Users must minimize the amount of Confidential Information provided and remove or anonymize any identifying or sensitive details wherever possible.

4.4.3. Without limiting the foregoing, AI Output must not be used in final work product, public-facing materials, communications, recommendations, reports, or decision-making processes unless it has been appropriately reviewed for accuracy, bias, confidentiality, intellectual property issues, and compliance with applicable law and Town policy.

4.5. **Ownership of AI Output**

Any AI Output generated using AI in the course of performing job duties for the Town will be owned by the Town, subject to any applicable agreement with a contractor or other third party. Users must not assume that AI Output is free from third-party rights and must ensure that any use of such AI Output does not infringe the intellectual property or other rights of any third party.

4.6. **Confidential Information, Personal Information, or Highly Sensitive Information**

4.6.1. The input of any Confidential Information, Personal Information, or Highly Sensitive Information held by the Town into any AI Tool is strictly prohibited.

4.6.2. Notwithstanding the foregoing, Confidential Information may be entered into an Enterprise AI tool only where: (a) the Enterprise AI tool has been expressly approved by the Town for that purpose; (b) the proposed use is within the scope of the applicable approval and any conditions or restrictions set out in Schedule "A" or otherwise by the Town; and (c) all applicable safeguards required by the Town are in place and followed.

4.6.3. Users must not enter Confidential Information, Personal Information, or Highly Sensitive Information into any AI Tool that is not expressly approved by the Town for the relevant category of information and use case. Users must also not use any AI Tool in a manner that causes Town data, Prompts, AI Outputs, or usage information to be retained, disclosed, or used for model training or service improvement, except to the extent expressly authorized in writing by the Town.

4.6.4. Users must not use any AI Tools to create non-personal data. Non-personal data may only be created in accordance with the Town's Non-Personal Data Policy.

4.7. **Disclosure, Monitoring and Reporting**

4.7.1 Users must comply with any Town requirements for logging or disclosing the use of AI, as may be established and updated by the Town from time to time. At a minimum, Users must disclose the use of AI where it is used to prepare materials that are shared externally or relied upon for operational or decision-making purposes. The Town may monitor the use of AI for security, compliance, and operational purposes. Any such monitoring will be conducted in accordance with the Town's applicable information technology, privacy, and security policies and applicable legal requirements.

4.7.2 Users must immediately notify the Town of any breach of this policy (*e.g.* if Confidential Information is entered into AI) or any unusual, suspicious, or unauthorized activity. Users must also promptly report any suspected issues relating to AI use, including unauthorized access, inaccurate or harmful AI Output, bias or discriminatory AI Output, intellectual property concerns, security concerns, or other non-compliance with this policy.

4.8. **Compliance**

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment, and, where appropriate, legal action. Contractors and other non-employees may be subject to contractual remedies, including suspension or termination of access to AI Tools or termination of their engagement, as applicable.

5. **Review and Updates**

This policy will be reviewed periodically by the Town and may be updated from time to time. Any updates will be communicated to relevant Users.

_____

Chief Administrative Officer

_____

Date

Schedule A: Approved AI Tools, Conditions, and Restrictions

Tier 1 – Enterprise AI Tools: Microsoft Copilot (M365).

- **Mandatory Requirement**: Users must have an assigned and active Town-issued Microsoft Copilot licence to use Copilot with any Town information. Use of Copilot without an assigned licence is not permitted.
- **Conditions of Use**: must be accessed through a licensed Town Copilot account; must be used within the Town's M365 tenant environment; must comply with data classification requirements; subject to monitoring, logging, and audit; users must complete required training.
- **Permitted Use Cases**: internal drafting, summarization, and analysis; productivity and internal communications; processing of information in accordance with classification rules.

Tier 2 – Public AI Tools: ChatGPT (non-enterprise), Claude (non-enterprise), Google Gemini (non-enterprise), and Perplexity (non-enterprise).

- **Conditions of Use**: Public Information only; no Internal, Confidential, or Restricted Information; must not be used to store or process Town data; must not be used for sensitive work.
- **Permitted Use Cases**: general research; public content drafting; external information gathering.

Tier 3 – Unapproved AI Tools: all other AI Tools not listed above are prohibited for Workplace Use. This includes, but is not limited to, browser extensions, plug-ins, aggregators, tools that capture or process data outside Town-controlled environments, or tools that violate Town policy, applicable law, or the Town's contractual obligations.

POLICY ON THE USE OF AI IN THE WORKPLACE – ACKNOWLEDGMENT FORM

I, _____ (employee name), acknowledge that I have read, understood, and agree to abide by the Town's Policy on the Use of AI in the Workplace. If I have any questions regarding this policy, I agree to contact the HR Department and/or my manager. I understand that the Town may change or amend this policy at any time. I also understand that if I violate any provision of this policy, I may be subject to disciplinary action, up to and including termination of employment, and that violations of this policy, including misuse of Town or third-party information, may also result in legal consequences. I further acknowledge that I am responsible for complying with any approval conditions, training requirements, recordkeeping requirements, and restrictions applicable to any approved AI Tool that I am authorized to use.

_____ _____

Employee's Signature Date

_____ _____

Town of Strathmore Date

TOWN POLICY

Strathmore

POLICY NUMBER: 1215

RESOLUTION NO.:
Resolution No. 156.05.26

ADOPTED BY:
Council

PREPARED BY: Strategic, Administrative & Financial Services

DATE: May 20, 2026

TITLE: Town of Strathmore's Video Surveillance Policy

Policy Statement

The Town of Strathmore recognizes the need to balance an individual's right to privacy and the need to ensure the safety and security of municipal employees, clients, visitors, and property. As an institution governed by the *Access to Information Act*, R.S.A. 2024, c. A-1.4 and the *Protection of Privacy Act* , R.S.A. 2024, c. P-28.5 the Town has obligations with respect to notice, access, use, disclosure, retention, and disposal of records. While video surveillance cameras are installed for security and law enforcement purposes, the Town's video surveillance systems must also be designed to minimize privacy intrusion. Proper video surveillance, where deemed necessary, is one of the most effective means of helping to keep Town facilities and properties operating in a way that protects security and privacy. Personal information collected by video surveillance includes video images and audio and must be protected from the risk of unauthorized access, collection, use, and disclosure.

This policy establishes procedures to achieve a balance between the purposes of and need for video surveillance and an individual's right to privacy, specifically:

- The operation of video surveillance at Town facilities;
- The use of information obtained through video surveillance at Town facilities; and
- Custody, control, access to, and retention of information created through video surveillance at Town facilities.

1.0 TITLE

1.1 This policy shall be cited as the "Town of Strathmore's Video Surveillance Policy".

2.0 DEFINITIONS

2.1 **Access to Information Act** or **ATIA** means the *Access to Information Act*, R.S.A. 2024, c. A-1.4, and any amendments thereto.

2.2 **Authorized Personnel** means the CAO, ATI Head, ATI Coordinator, POPA Head, the POPA Officer, or an approved and appointed Information Technology Technician for the Town of Strathmore.

2.3 **Chief Administrative Officer or CAO** means the principal staff person responsible for organizational performance who is appointed to the position of Chief Administrative Officer in accordance with the *Municipal Government Act* for the Town of Strathmore.

2.4 **Department Heads** means the CAO/Directors and any Managers who may be appointed to the Senior Leadership Team by the CAO from time to time.

2.5 **Director** means the individual in the Director role for the Town of Strathmore that oversees a specific department.

2.6 **Disclosure** refers to the release of relevant information. Disclosure includes viewing a recording as well as making a copy of a recording.

2.7 **Employees** means staff members of the Town of Strathmore whether permanent, full-time, part-time, or casual.

2.8 **Information Technologist (IT) Technician** means an IT Technician employed by the Town of Strathmore and is the individual responsible for downloading or redacting images requested by an Authorized Personnel.

2.9 **Law Enforcement** has the same meaning as defined in the *Access to Information Act* and the *Protection of Privacy Act*.

2.10 **Protection of Privacy Act** or **POPA** means the *Protection of Privacy Act* , R.S.A. 2024, c. P-28.5, and any amendments thereto.

2.11 **Storage Device** refers to a hard drive, computer disk or drive, CD ROM or computer chip used to store the recorded visual images captured by a surveillance system.

2.12 **Security Purposes** means an action or program that relates to public safety, the protection of the public or the deterrence or detection of criminal activity, including theft, vandalism, fire, or other property damage. This further includes the investigation of security incidents and environmental hazards, which or are suspected to have occurred.

2.13 **Video Surveillance System** refers to a mechanical or electronic system or device that enables continuous video recording, observing, or monitoring of space. This includes live video monitoring.

3.0 PURPOSE

3.1 The purpose of this policy is to regulate the use of video surveillance and recording on Town owned property and ensure that the collection, use, and disclosure of information complies with the *Access to Information Act* and the *Protection of Privacy Act*. This policy will ensure the consistency of Town of Strathmore surveillance measures and that information obtained through video surveillance will be used for Security and Law Enforcement purposes, pursuant to information sharing agreements.

4.0 APPLICATION

4.1 Access to Records

Access to the video surveillance records, e.g., remote access using the internet, CD, hard drives, etc., shall be restricted to Authorized Personnel. Two Authorized Personnel shall be present when surveillance records are accessed.

Information Technology staff will access the equipment only for the purpose of maintaining, backing up the software, and assisting with the extraction of the portions of the data. Cellphones will not be used to record the video surveillance footage. Surveillance records will be accessed and/or viewed only for a Law Enforcement purpose or Security Purpose, including in in the following circumstances:

a. At the request of Law Enforcement or for a fire investigation;

b. An incident has been reported or is suspected to have occurred or an investigation is warranted in relation to law enforcement or security purposes;

c. An environmental hazard has been reported or is suspected to have occurred; or

d. Pursuant to an Access to Information Request or disclosure request as contemplated by this Policy.

4.2 Storage and Logbook

All storage devices that are not in use must be stored securely in a locked receptacle located in an access-controlled area. An electronic log will be kept with regards to the access and use of all video surveillance footage and each recording device for stored surveillance. Storage Devices or video will only be removed for the purposes for use and disclosure as set out in this policy. The log will include the name of the Authorized Personnel who accessed the footage, the date of the footage, and the date of access. The Authorized Personnel responsible for this task

will take control of the storage device/video in question and secure it in a sealed envelope with the time and date of the seizure and initials of the individual on the seal of the envelope.

4.3 Add, Change and Removal of Equipment

All electronic video surveillance equipment requiring an add, change or removal request must be submitted to the Town of Strathmore's Information Technology (IT) Department. Any changes that occur without prior approval may result in disciplinary actions up to and including termination of employment.

4.4 Disclosure: ATIA and POPA

An individual who is the subject of the information has a right of access to his or her recorded information under the *Access to Information Act* and the *Protection of Personal Privacy Act* . Access may be granted in full or part depending upon whether any of the exceptions in the Acts apply and whether the excepted information can reasonably be severed from the record. All Access to Information requests for video records should be directed to the Legislative Service Department at the Municipal Office - 1 Parklane Drive, Strathmore, AB T1P 1K2 for processing. Access to Information Request forms are available at Town offices and on the Town's website. When a surveillance record is viewed by an individual who has requested access to his or her own information, the identity of any other person shown in the record will be obscured. The IT department will give access to Legislative Services for the requested video within 3 business days to review.

4.5 Disclosure: Law Enforcement

If access to a video surveillance record is required for the purpose of a Law Enforcement investigation, the requesting Officer must complete the Access to Information Request form and forward this form to the Legislative Services Department.

4.6 Information Sharing Agreements

The Town may enter an information sharing agreement with other public bodies where there is video surveillance of joint-use facilities. The terms of any information sharing agreement must be consistent with the purpose of this Policy and the provisions of the Acts. The Town may disclose video surveillance records in accordance with an Information Sharing Agreement, as provided for in the Acts.

4.7 Custody, Control, Retention, Disposal of Video Records/Recordings

The Town retains custody and control of all original video records not provided to Law Enforcement. Video records are subject to the collection, use, and disclosure requirements of the Acts, which includes, but is not limited to, the prohibition of all Staff from access or use of information from the video surveillance system, its components, files, or database for personal reasons. Except for records retained for criminal, safety, or security investigations or evidentiary purposes, or as

otherwise required by law, the Town must not maintain a copy of recordings for longer than 30 days unless otherwise specified in another contract or agreement. Any records that are accessed or disclosed in accordance with this Policy will be retained for one year.

4.8 **Unauthorized Access and/or Disclosure (Privacy Breach)**

Staff who become aware of any unauthorized disclosure of a video record in contravention of this Policy and/or a potential privacy breach are to immediately notify the ATI Head and POPA Head.

4.9 **Signage**

It is a requirement of the *Access to Information Act* and the *Protection of Privacy Act* that individuals be notified when the Town collects their personal information. Accordingly, at each facility where video surveillance takes place, signs must be prominently displayed at entrances to and egresses from the facilities. Any sign displayed must be easily observable to anyone who may be captured by the surveillance system, provide notice that the facility is under video surveillance, and identify the party who can answer questions about the surveillance system, including a contact number.

4.10 To respect the privacy of others, individuals will be notified with appropriate signage prior to entering any Town facility locker room, change room or washroom that no videotaping or photography will be tolerated as per this policy.

5.0 RESPONSIBILITY

5.1 The Chief Administrative Officer is responsible for the overall video surveillance policy. This responsibility may be designated to the ATIA and POPA Head.

5.2 The Department Heads are to ensure the requirements of this Policy are adhered to and must provide to the CAO or their designate a list of all facilities where video surveillance is in operation and where Storage Devices are kept. They will also ensure only Authorized Personnel are to access Storage Devices for a particular area.

5.3 Only Authorized Personnel are to access storage devices for a particular area.

5.4 Employees will review and comply with this Policy in performing their duties and functions related to the operation of a surveillance system. Failure to adhere to this policy, including the unauthorized access of video surveillance and Storage Devices, may result in disciplinary actions up to and including termination of employment.

5.5 Service providers will be accompanied by an IT Technician when required for any service requests, changes, additions, or deletions to the video surveillance.

5.6 Service providers having access to video surveillance information must sign a confidentiality agreement limiting access to, copying and disclosure of personal information and requiring compliance with this Policy. Breach of the confidentiality agreement may lead to penalties up to and including contract termination.

6.0 RELATED DOCUMENTS

6.1 *Access to Information Act*

6.2 *Protection of Privacy Act*

6.3 Service Alberta "Guide to Using Surveillance Cameras in Public Areas"

6.4 Video Surveillance Camera Locations

6.5 TOS Retention Schedule

6.6 Office of the Privacy Commissioner of Canada "Protecting and Promoting Privacy Rights"

END OF POLICY

APPROVAL

Mayor

Director of Strategic, Administrative and Financial Services

Schedule "G"

RECORDS MANAGEMENT BYLAW

BYLAW NO.17-13
TOWN OF STRATHMORE
IN THE PROVINCE OF ALBERTA

BEING A BYLAW OF THE TOWN OF STRATHMORE IN THE PROVINCE OF ALBERTA, TO PROVIDE FOR THE MANAGEMENT, RETENTION AND DISPOSITION OF MUNICIPAL RECORDS AND DOCUMENTS.

WHEREAS Pursuant to Section 214 (2) of the *Municipal Government Act,* R.S.A, 2000. Chapter M-26 as amended, a council may pass a bylaw respecting the destruction of records and documents of the municipality;

AND WHEREAS Section 38 of the *Freedom of Information and Protection of Privacy Act,* R.S.A. 2000, c.F-25, as amended, requires the head of a public body to protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction;

AND WHEREAS, it is the desire of the Town of Strathmore to provide regulations regarding the retention and disposal of records in the custody and control of the Town of Strathmore.

NOW THEREFORE THE MUNICIPAL CORPORATION OF THE TOWN OF STRATHMORE, IN COUNCIL ASSEMBLED, ENACTS AS FOLLOWS:

1. TITLE

1.1 This Bylaw may be cited as the "Records Retention Bylaw".

2. DEFINITIONS

2.1 In this Bylaw, unless the context otherwise requires:

a) **"CAO"** means the chief administrative officer of the Town of Strathmore or his delegate;

b) **"Disposition"** means:

the destruction of Records, or

the permanent retention of a Record once it has reached the end of its life cycle;

c) **"Personal Information"** means personal information as that term is defined in the *Freedom of Information and Protection of Privacy Act,* R S.A. 2000, c.F-25, as amended or replaced;

d) **"Record"** means a record of information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.

3. DISPOSITION AND RETENTION

3.1 Records in the care and custody of the Town are the property of the Town.

3.2 Disposition and storage of all Town Records must be in accordance with the Town Records Management Policy and Procedure.

3.3 If an individual's Personal Information will be used by the Town to make a decision that directly affects the individual, the Town shall retain the Personal Information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.

4. POWERS OF CHIEF ADMINISTRATIVE OFFICER

4.1 The CAO shall have the power and authority to:

(a) approve a Records Management Procedure, which addresses the, standards or guidelines relating to records management for the Town. The Records Management Procedure shall include a retention schedule to provide for the systematic control of the creation, use, maintenance, storage, security, retrieval, and disposition of records created or received by the Town in the conduct of its operations. The retention schedule shall also identify the retention period during which documents and records must be retained before Disposition;

(b) authorize the destruction of original copies of Records prior to the time outlined in the Records Management Procedure if those originals have been converted to electronic format that will enable copies of the original to be made; and

(c) authorize the retention of Records longer than the period provided for in the Records Management Procedure and shall do so where the Town has received an indication that there is or may be any litigation involving any of the said Records.

5. ENACTMENT

5.1 This Bylaw comes into full force and effect upon third and final reading.

READ A FIRST TIME this 7th day of February, 2018

READ A SECOND TIME this 7th day of February, 2018

READ A THIRD AND FINALTIME this 7th day of February, 2018

MAYOR

CHIEF ADMINISTRATIVE OFFICER

TOWN POLICY

POLICY NUMBER: 1701

REFERENCE:	**ADOPTED BY:**
	Town Council
Council 771.09.90	19 September 1990
Council 046.02.18	7 February 2018
PREPARED BY: Legislative Services	**DATE:** 7 February 2018

TITLE: RECORDS MANAGEMENT POLICY

POLICY STATEMENT

Advances in the Town's information technology strategies and changes in the electronic world now affect records and document management. With the advent of the Town's official electronic records management system, the need for a specific Records Management Policy addressing non-electronic and electronic records and information has become apparent.

2. DEFINITIONS

2.1 **"Archival Records**" An archival record is a record that has been reviewed for permanent retention because of its historical, fiscal, legal, operational or administrative value.

2.2 **"Retention Schedule"** This schedule describes the records under the custody and control of the Town of Strathmore, specifies how long the records must be kept as they progress through the phases of their life cycle, and what their final disposition will be at the end of their life cycle.

2.3 **"Convenience Copy"** means a printed or stored copy of the official record used for ease of reference that is not altered from the master records. Such records are transitory in nature and can be discarded when no longer useful.

2.4 **"Disposition"** refers to actions taken with regard to Town Records that have reached the end of their life cycle. This could be destruction, or permanent retention.

2.5 **"Electronic Document Management System" (EDMS)** EDMS is a software system for organizing and storing different kinds of digital documents.

2.6 **"Electronic Record"** An Electronic Record is information that is recorded or stored on any medium in or by a computer system or other similar device and can be read, reproduced, or perceived by a person or a computer system or other similar device.

2.7 **"Electronic Signatures"** An Electronic Signature consists of one or more letters, characters, numbers or other symbols in digital form incorporated in, attached to or associated with an electronic document.

2.8 **"Freedom of Information and Protection of Privacy Act, R.S.A. 2000, c. F-25, as amended (FOIPP)"** Alberta legislation, which provides the public with a right of access to Records held by the Town of Strathmore as a public body and protects the privacy of personal and sensitive information.

2.9 **"Naming Conventions"** Naming conventions for Documents and Records are a set of standard rules and formats to assist in their subsequent retrieval and handling.

2.10 **"Official Record"** The most complete record of an action, transaction or decision. It is the records that you rely on to take action and make decision. The official record is the complete record maintained in the electronic system.

2.11 **"Personal Information Bank"** A Personal Information Bank (PIB) is a directory list of the types of personal information held by the Town as a public body.

2.12 **"Record"** A Record is information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records.

2.13 **"Transitory Documents"** Transitory documents are document that have temporary usefulness and are only required for the completion of a routine action, or the preparation of another document or record.

2.14 **"Vital Records Program"** A Vital Records Program identifies and protects records containing vital information necessary for an organization to continue its key functions and activities in case of an emergency/disaster.

3. OVERALL PROGRAM

3.1 The Records Management Program ensures that all information assets, regardless of media or format, will be managed in a cost effective and efficient manner, while fulfilling all legal, archival, operational and fiscal requirements.

3.2 The records management program incorporates the following functions:

- Manage physical, electronic and inactive boxes
- Easy retrieval and search
- Email integration for emails that are declared records
- Class and metadata
- Consistent naming conventions
- Identification of vital records
- Retention Schedule and legal holds
- Permissions including deletion of records and access
- Workflows
- Version control and duplicate entries

4. RESPONSIBILITIES

Chief Administrative Officer

4.1 The CAO approves the Records Management Procedure and Retention Schedule.

4.2 The CAO must authorize the destruction of original copies of records as outlined in the Records Management Procedure.

Department Heads

4.3 All Department Heads are responsible for ensuring that each Town department is adhering to the Records Management Policy and Procedure.

4.4 All Department Heads are responsible for approving applicable Notice of Eligibility for Destruction of Records Requests.

Manager of Legislative Services

4.5 The Manager of Legislative Services is responsible for overseeing the Records Management Program including retention of records, destruction of records, security and storage of records and the classification and maintenance of all vital records.

All Employees

4.6 All Employees must ensure that Town records are placed in the Town's official electronic records management system to ensure that records are protected and not destroyed or removed from the custody and control of the Town.

4.7 All Employees are responsible for maintaining and filing of all documents created. Employees must not remove records in the custody and control of the Town from Town premises unless such removal is required to conduct Town business.

4.8 All Employees must abide by the Records Management Procedure attached hereto which provides direction and guidance for the organization on all records management procedures.

5. ELECTRONIC RECORDS

5.1 Electronic records, including e-mails are handled in the same manner as paper records. The class structure and retention schedule should be followed when handling electronic records and e-mails in the identical way that paper records are handled. Any changes to the class structure in the EDRMS will be done by a change management form.

6. SECURITY

6.1 All records must be handled in a secure manner. Wherever possible, file cabinets shall be locked after regular business hours. Any records containing personal or confidential information must be kept under lock and key.

6.2 Security has been built into the records management software program to ensure appropriate access for staff. A change management form must be used for any changes to security in the EDRMS.

7. STORAGE

7.1 Responsibility for the security and storage of all Town documents shall be the jurisdiction of the Manager of Legislative Services. The orderly and guaranteed safe storage of Town documents shall be provided by the implemented filing systems, the identification and protection of essential records, archival documents and the fire protection of records as necessary.

8. RECORDS RETENTION AND DISPOSITION

8.1 To protect the interests of the Town, it is important to ensure that records are destroyed in an appropriate and secure manner. An annual date for the disposition process will be December 31st of each year. All confidential records authorized for disposal shall be physically destroyed, i.e. shredded.

8.2 The Disposition process will have the following steps:

a) The Notice of Eligibility for Destruction of Records Requests shall be distributed on December 1 of each year to each Department Head.

b) Each Department Head that receives a Notice of Eligibility can approve or reject the notice.

c) After approval from the Department Head, the CAO will authorize all Notice of Eligibility for Destruction of Records.

d) After CAO authorization is given, the Manager of Legislative Services will arrange for destruction of all authorized records. A certificate signed by the Manager of Legislative Services shall attest to the time and place of the destruction of the Records, and contain a detailed list of the Records destroyed.

e) Legislative Services shall keep an index of:

- Records destroyed and all certificates and authorizations;
- Records retained longer than the period provided in the schedule; and
- Records retained permanently.

f) The certificate and the index shall be retained by the Town on a permanent basis.

9. END OF POLICY

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
2	**Community and Protective Services**										
3	CPS	All Departments	0306	Grants	All records about grants from initial applications through to close of grant. Grants to fund capital projects fall under IDS- Capital Projects	E	E+7	Destroy	E= Expiry		
4	CPS	Aquatic Centre	**0202**	Accidents					See HR -Accidents		
5	CPS	Aquatic Centre	**0502**	Rentals	Contracts for rentals	C	C+7	Destroy			
6	CPS	Aquatic Centre	**0502**	Reports	Minor First Aid, Major First Aid, Theft/Loss, Refusal of Treatment	C	C+ll	Destroy			
7	CPS	Aquatic Centre /Youth Club	**0502**	Program registrations	Lessons for the Town, (School and Red Cross) Class lists, Skill Charts, Instructor notes, cancellations. Youth Files	C	C+7	Destroy			
8	CPS	Aquatic Centre/ Family Centre	**0502/0504**	Maintenance Records	Maintenance - evidence of the regular maintenance and inspections Records may include - Cleaning Checks, Mechanical Checklists, Water Testing, Hazard Checklist	C	C+7	Destroy			
9	CPS	Aquatic Centre/ Family Centre	**0502/0504**	**MSDS**	Material Safety Data Sheets (MSDS)	S	5+3	Destroy			
10	CPS	Community Events/ Admin	**0110**	Concerts, Special Events & Events	Records relating to organization of municipal events such as open houses, trade shows, Canada Day, Heritage Days	C	C+5	Destroy	Review for Historical Records		
11	CPS	Community Services	**0121**	Economic Development	Planning and activities related to promotion and expansion of The Town of Strathmore tax base and growth	C	C+lO	Destroy			
12	CPS	Community Services	**0121**	Economic Development Projects	Names Economic Development projects that produce records related to the project	E	E+lO	Destroy	E=End of Project		
13	CPS	Community Services		Waivers	Waivers for events (sports & photos)	E	E+lO	Destroy	E=End of Event		
14	CPS	FCSS	**0700**	Good Food Box Program/Frozen Meal Program	Order forms and Receipts	C	C+7	Destroy			
15	CPS	FCSS	**0700**	Home Support Client Files	Invoices, Statement Client Billing Sheets	C	C+7	Destroy			
16	CPS	Fire Department	**0201**	Emergency & Disaster Plan	Emergency and Disaster Plan, Emergency Events	C	P	Retain		**X**	
17	CPS	Fire Department	**0201**	Fire Pit Permits	Application and Approved Fire Permits. Permits are not transferrable between home owners or occupants upon sale or vacating rental units.	T	T+l		T= Sale of House or vacating rental unit		By-Law 05-02

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
18	**CPS**	Fire Department	**0201**	Fire Reports	Includes photos as related to either a Motor Vehicle Accident or Fire investigation records. Fire Call information such at times and dates, witness statements, dispatch reports, Fire Commissioner reports, investigation notes and findings, anything pertaining to a fire. The paper records/reports done by the Fire Fighters after a call. Alarm Calls attended (False alarm, Smoke alarm, etc.) Public Events attended such as fireworks, stampede, parades, etc. Public Education Records (School visits either to the Fire Hall or at the school, Fire Hydrant training either at Fire Hall or at business location)	**C**	p	Retain			
19	**CPS**	Fire Department	**0201**	Fire Safety Inspection	Fire Safety Inspection reports	E	**E+2**	Destroy	E=Life of Facility		
20	**CPS**	Fire Department	**0201**	Personnel Files	Current SFD Members - Records include copy of driver's, boat, vehicle licenses, copies of all their training records, medals awards or corrective actions.	**C**	p	Retain	Kept at the Fire Hall	**X**	
21	**CPS**	Fire Department	**0201**	Pre-Post Inspection Books	Binders for pre-post inspection reports	**C**	C+7	Destroy			
22	**CPS**	Youth Club	**0506**	Financials					See Finance - Audited Financial Statements		
23	**CPS**	Youth Club		Raffle Records	Including all sold/unsold tickets, tickets inventory control sheets, list of prize winners	E	**E+2**	Destroy	E- After the last draw dates		AGLC Regulations
24	**CPS**	Youth Club	**0506**	Staff Files					See HR - Personnel		
25	**CPS**	Municipal Enforcement	**0210**	Enforcement Ticket - Bylaw	Bylaw Tickets	**C**	**C+5**	Destroy		**X**	Peace Officer Reg **AR312/2003** S16(a)(b)
26	**CPS**	Municipal Enforcement	**0210**	Enforcement Ticket - Provincial	Provincial Tickets	**C**	**C+5**	Destroy			
27	**CPS**	Municipal Enforcement	**0210-12**	Taxi	Taxi Licence - Records relating to the issuance and maintenance of taxi licences including mechanical inspections and permits	E	E+5	Destroy	E= close		
28	**CPS**	Municipal Enforcement/ Administration	**0103**	Citizen Complaints	Citizen Complaint forms	E	E+3	Destroy	E=Resolution of Complaint		Peace Officer Reg **AR312/2003** S16(a)(b)

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
29	CPS	Municipal Enforcement	**0210**	Municipal Enforcement-Forms, Letters, Certificates	Tow Forms, Calgary Humane Society Letter, Citizen Communication, Condo Letter, Certificate Radar Tuning fork test certificate	C	C+S	Destroy			Peace Officer Reg **AR312/2003** S16(a)(b)

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
30	**Corporate Services**										
31	CS	All Departments		Purchase Orders		E	E+7	Destroy	E= Completion		
32	CS	Assessment	0303	ARFI- Assessment Request for Information	Request for Information on Income and Sales property	C	p	Retain			
33	CS	Assessment	0303	Assessment Rolls		C	p	Retain		X	
34	CS	Finance		Account Receivable	Accounts Receivable records that are evidence of receiving, invoicing, processing and balancing monies owed to the Town. Records many include, collection of taxes, utilities paid and {TIPP) Tax Instalment Payment Plan. Cash receipts, Dog tag register.	C	C+7	Destroy		X	
35	CS	Finance		Accounts Payable	Accounts Payable records that are evidence of paying and reconciling monies owned by the Town including generating cheques, transferring funds Insurance.	C	C+7	Destroy		X	
36	CS	Finance	0301	Audited Financial Statements	Annual Audited Financial statement	C	p	Retain		X	
37	CS	Finance	0355	Banking	Included records that are evidence of banking activities. Records may include: bank reconciliation, bank statements, deposit slips and cheques	C	C+7	Destroy	Income Tax Regulations, C.R.C., c. 945, art. 5800		
38	CS	Finance	0356	Borrowing	Includes records that are evidence of borrowing and monitoring of debts. Records includes Debentures, debt payments schedules	C	p	Retain			
39	CS	Finance	0356	Budgeting	Included records that are evidence of the prepartation and maintanance of budgets. Records may inlclude: Working papers, summaries, budget presentations. Final Approved Operating and Capital Budgets are Permanent	C	C+7	Destroy			
40	CS	Finance		Finance, other	Any records that do not fit within the specified Finance categories above	C	C+7	Destroy			
41	CS	Finance		Financial Accounting	Includes records that are evidence of reviewing and posting activities for corporate transaction into the accounting system. Records may include Journal entries and correction and corporate transaction	C	C+7	Destroy			

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
42	CS	Finance		General Ledger	Records relating to the Town's general financial ledger. Includes Audit - Finance, General ledgers, (Annual reports and Annual Financial reports)	C	p	Retain			Income Tax Regulations, C.R.C., c. 945, art. 5800
43	CS	Finance	0306	Grants	All records about community and other grants to other parties	E	E+7	Destroy	E= Expiry		
44	CS	Finance	0600	Handi-Bus	Financials	C	p	Retain	Handi-Bus Records fall under the Handi-Bus board		
45	CS	Finance	0302-02	Insurance	Records relating to claims	E	E+12	Destroy	Municipal Affairs - Retention and Scheduling of Municipal Records E= After Settled		
46	CS	Finance	0302	Insurance	Certificate of Insurance	C	p	Retain			
47	CS	Finance	0302	Insurance - Claims	Records relating to insurance claims and records	T	T+ll	Destroy	T=Claim Closure		Limitations Act RSA 2000 Chapter L-12 Sec 3(1)(b)
48	CS	Finance		Investments	Town investment of funds	E	E+7	Destroy	E= Expiry		
49	CS	Finance		Journal Entries	Including General Posting Journals, Bank Deposit Posting Journals	C	C+7	Destroy			
50	CS	Finance		Reserve Funds	Reserve funds, reserve, replacement reserves, history	C	C+7	Destroy			
51	CS	Finance	0305	Taxes - School Declaration	Records related to the collection and maintenance of school tax declarations (Public or Separate) as part of the assessment and taxation roll requirements including school support declaration forms	E	E+7		E= Title Change		
52	CS	Finance		TCA	Asset Management & Capital Projects	C	C+12	Destroy	PSAB/TCA		
53	CS	Finance		Utilities	Records include resident water reconnect and disconnects. Meter readings, reports, Utility Receipts	C	C+7	Destroy			
54	CS	Finance		Utilities Bills	Utilities bill reports copied from Diamond	C	C+l	Destroy	Convience Copy		

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
55	**Infrastructure & Development Services**										
56	**IDS**	All Departments	**0132**	Bids/Proposals - successful	Request for Information on Income and Sales Request for Proposals, Request for Quote, Requests for Information. Records should include, decision/evaluation documentation and successful proposal/bid document.	**C**	**C+12**	Destroy	Contracts should be reclassified under contracts Municipal Affairs - Retention and Scheduling of Municipal Records		
57	**IDS**	All Departments	**0132**	Bids/Proposals - Unsuccessful		**C**	**C+II**	Destroy	Keep all unsuccessful tenders for 10 years in case of civil litigation - Municipal Affairs - Retention and Scheduling of Municipal Records		
58	**IDS**	Infrastructure	**INFR**	Bio solid Management	Monitoring of bio solid waste	**C**	p	Retain			
59	**IDS**	Infrastructure	**INFR**	Capital Projects	Records relating to the planning, construction and implementation of capital projects including tender documents, as-built, planning and design documentation, contract documents, specifications, meeting and reports, inspections and correspondence	**C**	p	Retain			
60	**IDS**	Infrastructure	**INFR**	Construction Planning and Monitoring	Records may include: notifications of Construction Completion Certification (CCC) and Final Acceptance Certification **{FAC)**	E	E+S	Destroy			
61	**IDS**	Infrastructure	**INFR**	Effluent, Irrigation Records	Effluent, Irrigation Records - Flow records, daily reports, daily pumps and generator reports, daily water sample reports, maintenance log books, water licenses and approvals.	**C**	p	Retain			
62	**IDS**	Infrastructure	**INFR**	Engineering Drawing		**C**	p	Retain			
63	**IDS**	Infrastructure	**INFR**	Infrastructure Management	Records to include: Evidence of the management, planning for sustainability, maintenance and replacement of the Town's infrastructure and facilities through capital projects. Infrastructure Inspections (bridges)	S	**S+S**	Destroy			
64	**IDS**	Infrastructure	**INFR**	Maps	Base/ Contour	**C**	p	Retain	Municipal Affairs - Retention and Scheduling of Municipal Records		

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
65	**IDS**	Infrastructure	**0401**	Road and Sign Maintenance	Includes records that are evidence of maintenance and routine inspecting of roads and signs such as plowing, and sanding of roads, snow, removal, clearing, patching, painting of road marking. Also includes the installations, maintenance an inspecting of traffic signs, signals and the concrete program for sidewalks and curbs. Records may include: Copies of specification books, inspections.	**C**	**C+II**	Destroy			
66	**IDS**	Infrastructure	**INFR**	Waste Collection	Includes records that are evidence of the routine operation and administration of the Town's waste collection Records may include: Monthly reports, contracts and tenders, annual Waste Management Report, diversion rates	**C**	C+7	Destroy			
67	**IDS**	Infrastructure	**INFR**	Studies and Reports	Infrastructure assets, infrastructure planning reports and studies, Master Servicing Reports	**C**	p	Retain			
68	**IDS**	Infrastructure	**INFR**	Utilities Maintenance	Includes records that are evidence of routine operations, inspection, monitoring and preventative maintenance on the Town's utility infrastructure, regular sewer flushing and Utilities location. Records may included: work site location map, work order, project summary reports	**C**	C+7	Destroy			
69	**IDS**	Infrastructure	**EPCO-01**	Water and Waste Water Control	Includes records that are evidence of monitoring, maintaining and repairing water and waste water management system such as ensuring water quality meets requirements through testing and sampling, conducting maintenance on the water reservoirs. EPCOR manages Flow Records, daily reading reports, daily pump and generator reports, daily water samples reports, maintenance log books, water licenses and approvals, infrastructure inspections, hydrant inspections, condition assessments and reports, work orders and Out of Scope Requests	**C**	p	Retain			

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
70	**IDS**	Infrastructure	**INFR**	Water Licenses	Records to include: Water Licenses, registrations, Authority & applications. Authorization, Code of Practice and Ministerial orders	C	P	Retain			
71	**IDS**	Infrastructure		Water Licenses Reporting	Records to include: Abnormal Circumstances, Regulatory compliance reports and test, 0 & **M** Report, AEP monthly reports, AEP Annual Report, EPP Plan, Crop Irrigation Report	C	P	Retain			
72	**IDS**	Operations and Public Works	**INFR**	Equipment	Records relating to Equipment owned by the Town	E	E+5	Destroy	E= Life of Equipment		
73	**IDS**	Operations and Public Works	**INFR**	Equipment Warranties	Includes Equipment Warranties	**S**	**S+I**	Destroy			
74	**IDS**	Operations and Public Works	**0401**	Fleet	Trip Inspection Reports	**C**	**C+2**	Destroy	Retain for current month and 6 month immediately proceeding		Traffic Safety Act - Commercial Vehicle Safety Regulation - Alberta Regulation **AR 121/2009** Section 38(2)
75	**IDS**	Operations and Public Works	**0401**	Fleet Administrations	Includes records that are evidence of activities related to the administration, maintenance, licensing and disposition of vehicles and equipment. Also includes regular and scheduled maintenance and inspections. Records may include: Equipment check list, maintenance check list, pre/post trip inspection reports, commercial vehicle inspections, repair request form, work orders, and bill of sales.	E	**E+4**	Destroy	E= disposition of vehicle/ equipment Records kept in respect of that vehicles shall be retained for a period of 6 months from the date that the vehicle was retired or disposed of		Traffic Safety Act - Commercial Vehicle Safety Regulation - Alberta Regulation **AR 121/2009** Section 38(1)
76	**IDS**	Operations and Public Works	**INFR**	Work Requests/ Orders	Includes Work Requests/ Orders	E	E+5	Destroy	E= Date Close		
77	**IDS**	Parks	0502 to 0513	Facilities	Records Includes Designs - Parks and Facilities Ball Diamonds, Family Centre, Civic Centre, Town Hall, Lambert Centre, Curling Rink, Youth Centre, Tennis Courts, Field House, Skateboard Park, Includes Design	C	P	Retain			

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
78	**IDS**	Parks	**0514**	Parks Maintenance/ Design	Records includes - log books, inspection records, ice thickness reports, agreements, park planning and design documents	**C**	**C+11**	Destroy			
79	**IDS**	Parks	**0514**	Playground	Records relating to playgrounds: Compliance Certificates, playground inspection reports	**S**	**5+10**	Retain			

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
80	**Planning and Development**										
81	IDS	Planning and Development	PD	Annexations	Final Order	C	p	Retain		**X**	
82	IDS	Planning and Development	PD	Area Structure Plans	Final Plans	C	p	Retain	Final Plans to be stored in the Vault	**X**	
83	**IDS**	Planning and Development	PD	Area Structure Plans	Records relating to development of final area structure plan (Working Copies)	C	C+7	Destroy			
84	**IDS**	Planning and Development	PD	Building Files	Working copies then move to Property Files				No retention as file will be moved to Property Files		
85	**IDS**	Planning and Development	PD	Building Permits Stats		C	p	Retain	Electronic Copy		Historical Information
86	**IDS**	Planning and Development	PD	Building Permits Stats	Paper copy	C	**C+1**	Destroy	These are printed from the Electronic Copy		
87	**IDS**	Planning and Development	PD	Business License		T	T+S	Destroy	T-Expiry of License (Paper receipts can be re-generated through Diamond)	**X**	
88	**IDS**	Planning and Development	PD	Land Use- Bylaws	Records related to research for, drafting and passing of Land Use Bylaws and amendments including approvals an application for a change in land use zoning, submissions to Council, decisions by Council and supporting information.	C	C+7	Destroy	Bylaw to be retained in Legislative Services - Record of reports in council agenda		
89	**IDS**	Planning and Development	PD	Drawings/As Builts/ Engineering Plans		C	p	Retain			
90	**IDS**	Planning and Development	PD	Offsite Levies	Records related to calculation and distribution of offsite levies.	C	p	Retain		**X**	
91	**IDS**	Planning and Development	PD	Historical records	Historical information about a site	C	p	Retain	Historical		
92	**IDS**	Planning and Development	PD	Legal Files	Development Permits and Building Permits. Electrical, Gas, Plumbing and HVAC Permits, RPR, PSR and Inspections. Safety Codes - Fire Inspections	C	p	Retain		**X**	
93	**IDS**	Planning and Development	PD	Receipts for Permits		C	C+7	Destroy	(Paper receipts can be re-generated through Diamond)		
94	**IDS**	Planning and Development	PD	Legal Plan		C	p	Retain	Operational Document		
95	**IDS**	Planning and Development	PD	Subdivision Files	Document History, Applications, plans, notification to land owners & replies	C	p	Retain		**X**	

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
96	**Strategic and Adminsitrative Services**										
97	**SAS**	Administration	**0101**	Acts and Legislation		**S**	**S+S**	Destroy			
98	**SAS**	Administration	**0100**	Administration, other	Any records that do not fit within the specified Administration categories above	**C**	**C+S**	Destroy			
99	**SAS**	Administration	**0102**	Advertising/ Publications	Records about various publications produced by the town, brochures and promotional materials, Newspapers, Newsletters, News Release	E	E+S	Destroy/Retain	E= publishing date (*note- 1 copy of each publication to be retained for historical purpose)		
100	**SAS**	Administration	**0303-02**	Assessment Appeals (ARB)	Appeals to Assessment notices provided to property owners (Board files)	p	p	Retain			
101	**SAS**	Administration	**0115**	Associations and memberships	Records relating to Associations and memberships, membership information, seminars and conferences	**C**	**C+S**	Destroy			
102	**SAS**	Administration		Authorization Delegations	Letters and orders to pass signing authority to designated staff from authorized parties to others during absence, or by bylaw	**S**	**5+12**	Destroy		**X**	
103	**SAS**	Administration	**0100-26**	Business Plan	Organizational chart, Documents Strategic Planning, Goals and Objectives, Profiles and History, Image and Identify, Action Plan	**C**	p	Retain			
104	**SAS**	Administration	**0120**	Cemetery	Records on the planning, design and management of cemeteries including archival, historical records, registers, lot books, and maintenance	**C**	p	Retain		**X**	Alberta Cemeteries **Act RSA 2000**
105	**SAS**	Administration	**0121**	Cemetery	Paper and electronic plot records including burials, cremation, interment, certificates and permits	**C**	p	Retain		**X**	Alberta Cemeteries **Act RSA 2000**
106	**SAS**	Administration	**0106**	Census	Records related to conducting and reporting the municipal census	**C**	**C+12**	Destroy			
107	**SAS**	Administration	**0106**	Census	Final Census Report	**C**	p	Retain			
108	**SAS**	Administration	**0107/0114**	Committees and Boards	Records related to boards and committees. Includes minutes and agenda.	**C**	p	Retain			Historical Information
109	**SAS**	Administration	**0102**	Communication	Records of a general nature regarding marketing, and public relations	**C**	**C+4**	Destroy			
110	**SAS**	Administration	**0104**	Copyrights, Trademarks, Logo and patents	Copyrights, Trademarks, logo and patents held by the Town	p	p	Retain		**X**	Copyright Act, Patent Act
111	**SAS**	Administration		Disaster Recovery Events	Records resulting in an emergency event	**C**	p	Retain			

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
112	SAS	Administration	0113	Elections - Ballots and voting register	Records produced in the conducting and reporting of electronics and plebiscites as described in the Local Authorities Election Act	E	E+6 weeks	Destroy	E= Date of voting		Local Authorities Election Act RSA 2000 CH. L-21 S.101
113	SAS	Administration	0113	Elections - Nomination Papers	Records produced from nomination papers	E	E	Destroy	E- Election of new Council must retain all the filed nomination papers until the term of office to which the nomination papers relate has expired		Local Authorities Election Act RSA 2000 CH. L-21 5.34 (4)
114	SAS	Administration	0113	Elections - Results	Official Election Results and affidavit of witness for Destruction of Election materials	C	p	Retain			Historical Information
115	SAS	Administration	0112	FOIP	Completion of requests or commissioners findings. Includes request, findings, commissioners orders, abandon requests, original package of material, reporting	C	C+S	Destroy			FOIP - Section 35(B) Min 1 year after using information
116	SAS	Administration		Land Files	Development Agreements, Subdivision Agreements, FAC, CCC, Agreement of Sale, Letter of Authorization, Irrevocable Letter of Guarantee	C	p	Retain		**X**	
117	SAS	Administration	0133	Legal Proceeding	Legal Proceeding - Records regarding litigation involving the municipality such as claim settlements, judgements, court orders	p	p	Retain	Administrative Decision		
118	SAS	Administration	0133	Legal	Incorporation Documents, Founding and establishment of Town, related authorities and corporate entities, certificate of incorporation, corporate seal	**S**	p	Retain		**X**	
119	SAS	Administration	LIB	Library & Reference material	Catalog and reference material stored in TOS library	**S**	5+2	Destroy			
120	SAS	Administration		Municipality History & Facts		C	p	Retain			
121	SAS	Administration		Permits, Licenses	Permits and licensing issued to the Town by external authorities, including Registrar of Motor Vehicles (AMVIR)	E	E+12	Destroy	E= Expiry		
122	SAS	Administration		Petitions	Petitions received in accordance with MGS Petitions Standards	p	p	Retain	Administrative Decision		
123	SAS	Administration		Phone Lists and Directories	Records Regarding staff lists and contact lists	**S**	**S**	Destroy			
124	SAS	Administration	0117	Policies and Procedures	Policies and Procedures passed by council.	C	p	Retain		**X**	
125	SAS	Administration	0114-05	Proclamations	Included proclamations	E	E+l		E- Proclamation Closed Review for Historical Value		

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
126	**SAS**	Administration		Project Management	Records resulting from the planning and management of well-defined, named projects. Does not include capital projects	E	E+IO	Destroy	E=Expiry		
127	**SAS**	Administration	**0215**	**RCMP**	RCMP policing records excluding grants, funding contracts	**C**	**C+5**	Destroy	Review for Historical Records		
128	**SAS**	Administration	**0110**	Receptions/Special Events	Non Historic	**C**	**C+5**	Destroy			
129	**SAS**	Administration	**0112**	Records Management	Disposition records - Approval authorities	**C**	P	Retain			
130	**SAS**	Administration	**0112**	Records Management	File System (Vault) - Including File Classification Scheme, File Lists, Retention Schedule	**C**	S	Destroy			
131	**SAS**	Administration		Security	Management and control of Physical security of Town facilities, access control system, staff identification	**C**	S	Destroy		**X**	
132	**SAS**	Administration	**0100-25**	Staff Meetings	Records regarding various department	**C**	**C+5**	Destroy			
133	**SAS**	Administration	**0140**	Studies/Reports		**C**	P	Retain			
134	**SAS**	All Departments	**0130/0131**	Agreement/Contracts	Contracts with internal or external parties including grant agreement, provincial and other land leases supply and services. Also includes cooperative agreement between Strathmore and other bodies not of a financial nature such as MOUs, Mutual Aid Agreements, Utility and water agreements.	P	P	Retain	Administrative decision	**X**	
135	**SAS**	All Departments	**0100-23**	Surveys and Statistics	Includes Internal department surveys	**C**	**C+5**	Destroy			
136	**SAS**	Council	**0116**	Bylaws	Final copies of bylaws approved by council	**C**	P	Retain		**X**	MGA Section **214(1)**
137	**SAS**	Council		Council Committee of the Whole Meetings	Town council approved minutes and final agendas packages	**C**	P	Retain			MGA Section **214(1)**
138	**SAS**	Council	**0114**	Council Committees	Committee struck or appointed by council where the Town has an interest and they is a reporting to council. Minutes are recorded in official council agenda packages and minutes. Doesn't include Council Meetings or Committee of the Whole Meeting	C	P	Retain			
139	SAS	Council	**0114**	Council Meetings	Town Council approved minutes and final Agenda	C	P	Retain		**X**	MGA Section **214(1)**
140	SAS	HR	**0202**	Accidents	Records relating to accidents and incidents involving injury to people and/or damage to property.	E	E+12	Destroy	E=Completion of Investigation or settlement of claim Municipal Affairs - Retention and Scheduling of Municipal Records		Limitations Act RSA 2000 Chapter L-12 Sec 3(1)(b)

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

Schedule "I"
Town of Strathmore Retention Schedule - 2017

	A	B	C	D	E	F	H	I	J	K	L
1	**Division Code**	**Department**	**RM Code**	**Record Title/Series**	**Description**	**Active Years**	**Total Years**	**Suggested Disposition**	**Comments**	**Vital Record**	**Defining Authorities**
141	SAS	HR	HR	Investigation	Non OHS/WCB investigation, complaints and all related subsequent documentation	T	T+12	Destroy	(T- Close of investigation)		
142	SAS	HR	HR	Personnel	Employee Files - Containing Employee Contact, WCB, Benefits, Job Performance, Discipline, Training	C	C+7	Destroy	C= Current Employee - Active Employee (*Not Current Year).	**X**	
143	SAS	HR	HR	LAPP & APEX	Records related to LAPP and APEX	E	E+7	Destroy	E=All Pension Obligations Paid Out		
144	SAS	HR	HR	Recruitment	Files for Competition for the Town - Resumes and short list applicants paper responses	T	T+l	Destroy	(T-Close of competition) Successful applicant to be reclassified to Personnel records		
145	SAS	HR	HR	Staff Scheduling & Tracking	Time Sheets, Requests for Leave	C	C+7	Destroy			
146	SAS	HR	HR	Payroll Processing	Payroll Processing, Year End Payroll, Summaries, T4's, COLA and Payroll Registers	C	C+7	Destroy			
147	SAS	HR	HR	Year-End Payroll	T4, LAPP Report, Sun life Statement, Paper Timesheets, GL Code	C	p	Retain			
148	SAS	IT	IT	Application Software	Records relating to computer software including manuals, training information and correspondence	**S**	**S**	Destroy			
149	SAS	IT	IT	Asset Tracking	Hardware/ Software	E	E+l	Destroy	E= Disposal of Asset		
150	SAS	IT	IT	Back up	Contains backups of all servers	**S**	**S**	Over-written		**X**	
151	SAS	IT	IT	Council Video	Recorded Video of Council meeting	C	p	Retain	Historical		
152	SAS	IT	IT	Manuals for Equipment		**S**	**S**	Destroy			
153	SAS	IT	IT	Network Administration	Diagrams/Drawings	**S**	**S**	Destroy			
154	SAS	IT	IT	Passwords/ Credentials		**S**	**S**	Destroy			
155	SAS	IT	IT	Ticketing System	Requests/Tickets From the IT Help desk Ticketing System. Includes end user training, helpdesk, minor repairs support plans and support records	C	C+6	Destroy			
156	SAS	IT	IT	Video Security		**S**	**S**	Destroy	30 Days		
157	SAS	IT	IT	Web Administration	Records relating to the administration of the municipal website including layout and content as well as design development and maintenance	**S**	**5+2**	Destroy			
158	SAS	Maintenance	IT	Ticketing System - General Requests	Includes records - relating to the Maintenance ticketing system requests	C	C+6	Destroy			

Retention Trigger Event: Is the event that must occur before a retention period begins.
[C = Current Year End; P = Permanent; S = Superseded or Obsolete; T = Terminating Event E - Event Required Before calculating Retention]

POPA PIA Template Completion Guide

Disclaimer:

The content of this document is informational in nature and does not constitute legal advice.

Information is shared in accordance with Municipal Government Act and is managed in compliance with the Access to Information Act (ATIA) and the Protection of Privacy Act (POPA). If you have any questions about the Town's collection or release of information, please contact the Town of Strathmore's ATI Coordinator at 403-934-3133 or by email at ATIA@strathmore.ca.

Section 26 of the *Protection of Privacy Act* (POPA) requires a public body to prepare a privacy impact assessment (PIA) in prescribed circumstances and, if required by the regulations, submit the PIA to the Information and Privacy Commissioner in accordance with the regulations. In addition, as part of the Commissioner's responsibility to monitor how POPA is administered to ensure that its purposes are achieved, the Commissioner may, as described in section 27(1)(j) of POPA, request a copy of a public body's PIA.

Section 7(1) of the *Protection of Privacy Act* (Ministerial) *Regulation* (M-Regulation) lists the circumstances in which a public body must prepare and submit a PIA to the Commissioner.

This **POPA PIA Template Completion Guide** ("Completion Guide") is a companion document to the POPA PIA Template. The aim of this Completion Guide is to assist public bodies in completing the POPA PIA Template. This Completion Guide provides explanation or clarification, where necessary, for each question asked in the POPA PIA Template and describes what is expected of the public body in each question. We recommend that you complete the POPA PIA Template while consulting this PIA Completion Guide.
The term "**project**" when used in this document means any administrative practice, program or service, or a change to any existing administrative practice, program or service that a public body plans to implement, which will involve the collection, use or disclosure of personal information and which includes one or more of the factors listed in section 7(5)(a) to (e) of the M-Regulation.

If a public body is unsure whether it is required to complete a PIA or complete and submit a PIA to the Information and Privacy Commissioner, the public body should consider using the PIA Submission Assessment Tool to make that determination.

Please note that sections in the POPA PIA Template with an asterisk (*) are mandatory and must be completed. Any PIA that does not complete the mandatory sections, will be deemed incomplete and will not be accepted for review by the OIPC.

Note: Public bodies should not submit this completion guide to the OIPC as part of their PIA submission.

Given that section 26(1) of POPA requires a public body to prepare a PIA in prescribed circumstances and, if required by the regulations, submit it to the Commissioner in accordance with the regulations, the head of a public body is legally required to sign off on POPA PIAs. However, 55(1) of POPA authorizes the head of a public body to delegate to any person any power, duty or function of the head under the Act, except the power to delegate under this section. Section 55(2) requires that a delegation under subsection (1) be in writing and may contain any conditions or restrictions the head of the public body considers appropriate. To this end, the Designate of a public body may sign off on the public body's PIA if that Designate has been delegated such a power. A copy of the delegation of power should be included with the PIA.

Table of Contents

- A. General Information About the Public Body or Bodies, Existing PIAs, and the Project*
- B. Details About the Project*
- C. Information About Your Privacy Management Program (PMP)*
- D. Identify Personal Information Involved and Your Authority to Collect, Use or Disclose the Information*
- E. Access, Correction, Accuracy, Retention, Disposition*
- F. Protection of Information*
- G. Service Providers*
- H. Project Risk Assessment and Mitigation*
- Appendix A. Data Matching
- Appendix B. Common or Integrated Program or Service
- Appendix C. Use of Automated Systems or Other Forms of Innovative Technology
- Appendix D. PIA Cover Letter*
- Appendix E. PIA Submission Checklist*

A. General Information about the public body or bodies, existing PIAs, and the project *

Questions in this section are asked as a legislative requirement and to enable the OIPC in processing the PIA file.

Question 1

Section 26 of POPA requires The Town of Strathmore (The Town) to prepare a PIA in the circumstances listed in section 7 of the M-Regulation, when a project involves the collection, use or disclosure of personal information. If a public body is not collecting, using or disclosing personal information as part of its project, there is no requirement under POPA to submit a PIA to the Commissioner for the project.

Question 2

The legislation is clear on when The Town is required to prepare a PIA, and only in the prescribed circumstances as listed in the POPA PIA template is the Town required under POPA to submit a PIA to the OIPC. Please note that the list of highly sensitive information identified under section 1 of the M-Regulation is not an exhaustive list. Other personal information may be of high sensitivity.

In this question, if only the last checkbox (the loss of, unauthorized access to or unauthorized disclosure of the personal information could result in significant harm) is selected, the Town may not be required to submit a PIA to the Commissioner. Nonetheless, the OIPC recommends that public bodies use the POPA PIA template while preparing PIAs under section 7(1)(a) of the M-Regulation as the Commissioner may request copies of those PIAs under section 27(1)(j) of POPA. Using the template will ensure that the Town complete their PIAs in alignment with the PIA requirements under POPA and the M-Regulation of which the PIA template is based on.

Question 3

When submitting a PIA to the OIPC as required under section 26 of POPA, the OIPC needs to know certain information about the Town including who the head of the Town is at the time the PIA is submitted. This is because under POPA the head has specified duties including for protection of personal information (section 10(1)).

Question 4

Section 7(4)(b) of the M-Regulation allows for two or more public bodies to submit a PIA for a common or integrated program or service, hence the need to know if the PIA is for such a project.

Question 5

No additional explanation needed.

Question 6

No additional explanation needed.

Question 7

Sometimes, a new PIA is related to a PIA which has already been submitted to the OIPC and is still under review. In such cases, it is important that the OIPC is aware of this PIA to ensure the recent PIA is not reviewed in isolation from the related PIA. There are also times where information in an existing PIA is referenced in a new PIA. It is also important to know if such a PIA exists or has been previously reviewed by the OIPC.

Question 8

A PIA amendment addresses privacy and security risks associated with changes to an existing project that impacts the collection, use and/or disclosure of personal information. A PIA amendment focuses on areas that have changed in an existing project, and how the Town has identified and addressed privacy and security risks associated with the change. An amendment to a previously submitted PIA requires that the updated or new PIA is reviewed in consultation with the previously submitted PIA.

Question 9

Some public bodies have their own filing convention for their internal use. Providing this number ensures the OIPC, in addition to the OIPC's file number, references this number in its communication with the Town.

Question 10

This informs the OIPC whether the project under consideration has been implemented or not.

Question 11

This question aims to inform the Town which sections of the appendices to the POPA PIA template are relevant to their project as well as relevant resource expertise needed to assist the Town in completing the technical aspect of the PIA. The question also informs the OIPC what to consider regarding legislative requirements during the PIA review process as different projects may have unique compliance privacy and security issues to consider.

For projects that involve automated systems, section 7(3) of the M-Regulation states that a PIA must provide a level of detail commensurate with the complexity of the practice, program, project or service the PIA relates to. As such, the Town is required to also complete an Algorithm Impact Assessment (AIA). AIA is a tool used for identifying and addressing the risks and impacts of automated decision-making systems. Typically comprising of a set of questionnaires, the tool can be used to determine the impact level of an automated decision-making system including biases, human rights violations, ethical violations, marginalization and accessibility issues. The OIPC is in the process of developing an AIA tool. Once completed, it will be published on the https://oipc.ab.ca and a link to it will be added to the POPA PIA Template and this document. In the interim, the OIPC recommends that where a project involves automated systems, the Town consult industry standard algorithm impact assessment guidelines in preparing and submitting their AIAs with their PIAs.

B. Details About the Project*

Question 12

This information assists the OIPC in understanding the project, its business rationale and the purpose or objective it intends to achieve for the Town. This question also informs the OIPC on why the collection, use and/or disclosure of personal information is required by the Town to meet the needs of the project. It is imperative that the Town provides sufficient detail on the project. In addition, in this question, the Town is required to provide technical information about the project under consideration. For instance, if the public body is a police agency implementing a body worn camera (BWC), the public body is expected to describe each body worn camera unit, its associated features and IT infrastructure that operates the BWC. Also, information on BWC storage media, how information is transferred from the camera to the IT network, where information is stored and who is responsible for managing the information, etc. must be provided. In other words, the entire lifecycle of the personal information involved must be addressed in all aspects of the project. The Town should also consider attaching technical details of the project as necessary.

Question 13

An electronic information system has specific technical requirements, such as logging and auditing, access controls, that need to be considered and assessed to ensure the access and privacy rights of Albertans are upheld, which is why we need this information.

Question 14

Other stakeholders' involvement in a project may determine who is collecting, using or disclosing personal information in the project and as a result shed some light on how the Town ought to consider the legal authority for each stakeholder to collect, use and/or disclose personal information involved in the project.

C. Information About Your Privacy Management Program (PMP)*

Question 15

Section 25(1) of POPA requires the Town to establish and implement a PMP and make it public or provide a copy of the PMP upon request pursuant to section 25(5). These requirements will come into effect on June 11, 2026. The Town's policies and procedures must comply with the requirements of POPA and its regulations. The OIPC is working on issuing a POPA PMP Guideline which will be available on the OIPC website to assist the Town in meeting their PMP obligations under POPA.

Not having a PMP leaves a gap in the completion of the PIA. This could potentially lead to non-compliance. It is important to provide the OIPC PMP file number of the Town's most current PMP where applicable, as by doing so it saves the Town time and effort by referencing the already submitted PMP and avoids duplication. Also from a PIA review standpoint, it is relevant to review the PIA to assess the Town's compliance with applicable legislation.

D. Identify Personal Information Involved and your Authority to Collect, Use or Disclose the Information*

Question 16

This question ensures that the Town identifies the personal information that it intends to collect, use or disclose in the project. In doing so, the Town would have to start thinking about its legal authority to collect, use or disclose personal information and whether those authorities align with sections 4, 12 and 13 of POPA, respectively. In addition, the Town is required to consider the limitation principle under sections 12(4) and 13(4) of POPA. Under section 12(4) the Town needs to explain how the use of personal information in the project is **only to the extent necessary** to enable the Town to carry out its identified purposes in a **reasonable manner***.* Similarly, under section 13(4) of POPA, the Town needs to explain how the Town public disclosure of personal information is **only to the extent necessary** to enable the Town to carry out its identified purposes in **a reasonable manner**. Personal information means recorded information about an identifiable individual. Some examples of personal information include an individual's name, home or business address, home or business email address, race, gender identity, fingerprints and financial history. For a complete listing of what is considered personal information, please see **section 1(q) of POPA.**

Question 17

Section 5 of POPA provides for the manner of collection of personal information. It is important that the collection of personal information for this project meets the requirements of section 5 of POPA. In this question, the Town needs to consider and explain how section 5(2) of POPA is complied with in this project if personal information is collected directly from the individuals who, are the subjects of the information, including when and how a collection notice is provided to those individuals. In particular, the Town needs to explain whether section 5(2) of POPA applies to its project and how the Town complies with it.

Question 18

While there are legal authorities for the Town in POPA to use or disclose personal information, there are situations where the Town may rely on individuals' consent to use or disclose their personal information. Such consent must meet the prescribed requirements of section 2 of the Protection of Privacy Regulation ("the Regulation"). That is, the consent process for the project needs to clearly explain whether consent is obtained electronically or manually. Where consent is collected electronically, the Town should state how individuals give their consent. While a consent form is the implementation of the above consent requirements, the Town needs to have policies and procedures in place to collect and manage consent.

Question 19

There are circumstances where personal information can be collected indirectly, which means the collection comes from a source that is not the person whom the information is about. If that is the case in this project, this question gives the Town the opportunity to describe why, and how personal information is collected indirectly.

Question 20 – An information flow diagram is not the same as a business flow or a network diagram. An information flow diagram identifies the flow of specific pieces of information from one entity to another and when the entities involved are collecting, using or disclosing the information in question. It has arrows indicating the direction of flow of information between the entities. In some cases, information flow could be bi-directional between two entities. The information flows help in identifying the legal authority for collecting, using or disclosing personal information by each entity involved in the flow of the information. A network diagram depicts an IT network infrastructure or network segment and its associated components which may include, servers, routers, firewalls, databases, etc. A business flow diagram is a step-by-step process on how a specific business task is accomplished.

Question 21
No additional explanation needed.

E. Access, Correction, Accuracy, Retention, Disposition*

Question 22

This question is asked to remind the Town to ensure it takes steps to make individuals aware of their rights to request access to their personal information that is in the custody or under the control of the Town. Usually, public bodies should be transparent by making their access to information request processes public, with specific contact information of a person or business unit that handles access to information requests. In certain circumstances, the Town should make proactive disclosure to minimize the number of access requests they get.

Question 23
While this may be addressed as part of the PMP, the Town is required to have access request policies in place to ensure that Albertans can exercise their rights to access their information. Such a policy governs how the Town implements its access to personal information processes to ensure consistency in processing such requests.

Question 24

This question is asked to ensure the Town has established a process to make individuals aware of their right to request correction to their personal information involved in the project. Usually, public bodies should be transparent by making their correction to personal information request processes public with specific contact information of a person or business unit that handles correction requests.

Question 25

While this may be addressed as part of the PMP, the Town is required to have correction request policies in place that govern how Albertans can exercise their rights to correct their personal information and to ensure consistency in processing such requests.

Question 26

The Town has an obligation to make every reasonable effort to ensure that information about individuals that the Town relies on to make decisions that affect those individuals is accurate and complete.

Question 27

It is important to understand how the Town complies with section 6(b) of POPA for this project by ensuring that there exists a retention and disposition policy for information used in this project to govern how long personal information must be retained.

Question 28

Implementing record retention and disposition policies into information systems ensures that information that has reached its retention period is automatically flagged by the system for disposition instead of it being a manual process that is prone to inconsistencies and human errors resulting in information being retained past its retention period. Information held longer than its retention period poses a risk of loss, unauthorized access, or unauthorized disclosure.

F. Protection of Information*

Question 29

Information security classification means assigning security levels to information that are based on the sensitivity of the information in question. Classifying the information based on the Town's information classification standard assists the Town to protect the information by implementing security controls that are proportionate to the classification levels of the information. Each public body is required to implement an information security classification system to assist the public body to classify information that it collects, uses or discloses as required under section 2(1) of the M-Regulation. The Town must meet this requirement before submitting their PIAs to the Commissioner for review.

Question 30

The "reasonable security arrangements" standard set out in section 10(1) of POPA are determined by the security classification of the personal information involved in the project. If the security classification is high, then the security measures, i.e., the administrative, technical and physical safeguards, must be correspondingly high. Whereas, if the security classification is low, then fewer measures may suffice to meet the standard. Section 6(2(b) of the M-Regulation requires public bodies having custody or control of a high volume of personal information or highly sensitive personal information to have documented safeguards. POPA does not stipulate a threshold for "high volume" or "significant percentage of the population". The interpretation of this section of the M-Regulation is contextual in relation to the project. Although Section 1 of the M-Regulation deems certain personal information to be highly sensitive (biometric and financial information, and personal information of minors and seniors), this list is not an exhaustive or exclusive list. Other types of personal information may be deemed to be highly sensitive in specific contexts.

1. Administrative safeguards govern the implementation of other protective measures and ensures that such measures are implemented consistently during the life cycle of the project. Consistent implementation of protective measures reduces vulnerabilities usually caused by lack of good security governance.

2. No additional explanation needed.

3. The technical safeguards should directly protect the information involved in the project, not just the general technical safeguards implemented by the public body. For instance, access controls should be specific for the project and describe how such controls ensure only authorized individuals have the right level of access to information involved in the project. In addition, any security assessments results such as vulnerability assessment and penetration tests conducted specific to the project should be included as part of the public body's PIA submission, as such results provide additional information on risks that were identified and how they were resolved as part of the project implementation.

Question 31

Continuous assessment and monitoring of safeguards assist the Town in ensuring that the safeguards are working as expected. For instance, employees should be required to take refresher trainings on privacy and security. Also, monitoring controls such as intrusion detection and prevention systems should be implemented.

Question 32

Section 6(1)(b) of the M-Regulation requires the Town to establish policies and procedures that ensures they comply with the Town's obligations under POPA such as responding to incidents (unauthorized access to, unauthorized disclosure of or loss of personal information). Section 6(1)(d) of the M-Regulation also requires the Town to train their employees about the employee's obligations under POPA. As part of that training, the Town should make their employees aware of their obligations under POPA, which includes notifying the Town of incidents under section 10(2) of POPA.

Question 33

Access control policies ensure that access to the Electronic Information System (EIS) is consistently managed, including requests to access the EIS, account provisioning and revocation of account when an employee no longer needs access to the EIS. Through enforceable access control policies, the Town will be able to ensure that an employee only gains access to the information they require to perform their job functions.

If the project involves a high volume of personal information or highly sensitive personal information, a documented access control policy must be attached to the PIA submission. POPA does not stipulate a threshold for "high volume" or "significant percentage of the population". The interpretation of this section of the M-Regulation is contextual in relation to the project. Although Section 1 of the M-Regulation deems certain personal information to be highly sensitive (biometric and financial information, and personal information of minors and seniors),

this list is not an exhaustive or exclusive list. Other types of personal information may be deemed to be highly sensitive in specific contexts.

Question 34

Having an access requests process for the EIS ensures access requests are submitted by appropriate business heads for approval by the appropriate authority prior to processing and account provisioning. Each request should identify the permission level for employees requiring access and ensure the permission level gives the employee only the right access required for the specific job tasks.

Question 35

All access requests to the EIS must be approved by the appropriate level of management, to ensure that employees who access the EIS are authorized to do so.

Question 36

It is important to ensure that access to the EIS is revoked in a timely manner when employees no longer need such access, to prevent potential unauthorized access to personal information. It is also to ensure dormant accounts are removed from the system, as such accounts pose security risks.

Question 37

The access control table provides clarification on the access privileges of the users of the system including the kind of actions each user can take and what information the user can access, and how the permission limits users only to the information they need to perform their job tasks or functions. The Town's information technology (IT) department plays a significant role in implementing access controls in systems and will be a good resource for assisting in completing this table.

Question 38

Logging and auditing policies ensure that information systems are built and implemented to capture audit logs of activities that are occurring within the system, including unauthorized activities listed under section 10(2) of POPA. Such a policy also ensures proactive auditing of information systems to detect and manage incidents defined under section 10(2) of POPA.

If the project involves a high volume of personal information or highly sensitive personal information, a documented auditing and logging policy must be attached to the PIA submission. POPA does not stipulate a threshold for "high volume" or "significant percentage of the population". The interpretation of this section of the M-Regulation is contextual in relation to the project. Although Section 1 of the M-Regulation deems certain personal information to be highly sensitive (biometric and financial information, and personal information of minors and seniors), this list is not an exhaustive or exclusive list. Other types of personal information may be deemed to be highly sensitive in specific contexts.

Question 39

Being able to capture and maintain audit logs of personal information means that the Town can

identify and investigate unauthorized access to, unauthorized disclosure of, or loss of personal information in order to meet its obligations under section 10(2) and (3) of POPA and sections 4(3), (4) and (5) of the M-Regulation.

Question 40
Proactive auditing is a way of monitoring access to an EIS to detect and respond to potential unauthorized access to, unauthorized disclosure of, or loss of personal information.

Question 41
No additional explanation needed.

G. Service Providers*

Question 42
Given that service providers, which includes corporations, are considered employees under section 1(h) of POPA, the Town is accountable for the service provider's compliance with POPA. Therefore, it is important for the Town to consider privacy issues that may involve the service provider's role in relation to any personal information it may collect, use, disclose or access as an "employee" of the Town.

Question 43
If a service provider will have access to personal information as part of providing its services to the Town or if it will collect, use or disclose personal information on behalf of the Town, the Town must ensure it complies with POPA as it relates to these activities. Therefore, the contract with the Town must address all related compliance issues such that through the implementation of the terms of the contract agreed to between the Town and the service provider, the Town has confidence that the service provider will comply with POPA in providing its services concerning any personal information involved in service delivery. A service provider must also protect the personal information it has in its custody, or that it is otherwise responsible for, according to the terms of the contract which must ensure compliance with section 10(1) of POPA, i.e., the security of the personal information must at minimum align with the Town's security safeguards for this type of information. The agreement must also set out how the service provider interacts with the Town's privacy management program. Without an agreement that addresses all these compliance related issues, there is a risk of non-compliance by the Town as a result of the activities of its service provider. Consequently, as part of the PIA review, any agreement entered into with a service provider must be reviewed by our office as part of the PIA review process. This is because the service provider agreement plays a central role in determining whether the service provider-employee is positioned within the terms of the contract to comply with POPA. **Submitting a copy of the agreement with your PIA is a mandatory requirement**.

Section 7(6) of the M-Regulation provides that where the Town is required under POPA or the Regulation, to enter into an agreement relating to the practice, program, project or service the PIA relates to, the portions of the agreement relating to the protection of privacy must be submitted to the Commissioner together with the PIA. Under section 1(1)(h) of POPA, an

"employee" includes those providing a service to the Town "under contract." The contract with the service provider would demonstrate the Town's authority under POPA to share personal information with the service provider or otherwise permit it to collect, use or disclose personal information on its behalf. Therefore, it is an essential part of the PIA submission.

Question 44

A Town may delegate responding to access to information request responsibility to its service provider. However, the Town must ensure that its contractual agreement with the service provider adequately addresses access to information request processing and describe how the service will be provided to the Town.

Question 45

To ensure the Town is able to meet its obligations under POPA the Town must ensure it maintains control of the personal information involved in the project where this information is collected or accessible by the service provider. This is required to ensure the personal information remains subject to POPA and the *Access to Information Act* (ATIA) to preserve the rights of individuals concerning their personal information under these Acts. Failure to retain control of the personal information amounts to a disclosure, which is prohibited under POPA without authority for said disclosure. This means, that there is a high likelihood of a breach if the Town fails to retain control of personal information in an agreement and provides personal information to the service provider for the services. For this question, if the Town's answer is yes, the Town must identify specific sections of its contract with the service provider that ensures the public body maintains control of the information for the project. **Public bodies must meet this requirement before submitting their PIAs to the Commissioner for review.**

Question 46

For this question, refer to the information set out in the commentary above for Question 43.

Question 47

Service providers are considered employees of the Town and should have appropriate training prior to accessing personal information and continue to have refresher training for the duration of their contract. Section 6(1)(d) of the M-Regulation.

H. Project Risk Assessment and Mitigation*

This section of the PIA template requires public bodies to identify the project's privacy and security risks and associated administrative, technical and physical safeguards that address these risks. This completion guide provides some **example descriptions** of the types of risks identified in the POPA PIA Template risk table.

Question 48

Conducting security vulnerability assessments (VA) during the implementation of an information system that processes identifying information ensures exploitable security vulnerabilities or weaknesses are identified, prioritized and addressed in a timely manner**.** A penetration test

(pentest) is performed to test if security controls are working as expected. VA and pentest are part of an overall risk management strategy and should be conducted periodically. Other security assessments can also be conducted and included in the PIA. Providing copies of these assessments with your PIA goes on to demonstrate the Town's commitment to protect personal information pursuant to section 10 of POPA.

H1. General Risks (to be completed for all PIA submissions) *

Risk 1
E.g., personal information is collected by the Town and/or the information system is configured to accept personal information that does not relate directly to and is necessary for the project. Systems built for the global market have default configurations that allow for the collection of vast amounts of personal information. Such systems should be hardened by disabling data fields that are not required for specific project implementations to manage the risk of over collection.

Risk 2
E.g., information that was collected for this project is used for a purpose not directly related to the project, contrary to section 12 of POPA.

Risk 3
E.g., information that was collected for this project is disclosed contrary to section 13 of POPA. Personal information could be intercepted while in transit due to lack of appropriate security control, leading to unauthorized disclosure. There are also situations where the Town or its employees disclose personal information for secondary purposes without legal authority. Unauthorized disclosure could also be via insecure disposal of information processing media.

Risk 4
E.g., information collected for this project is accessed by unauthorized users or malicious software due to lack of reasonable safeguards, contrary to section 10(1) of POPA.

Risk 5
E.g., information collected for this project is lost as a result of human error or malicious software attacks, such as ransomware, which renders information inaccessible. This may lead to the inability of the Town to perform its business functions or respond to requests from individuals to access their information. Disgruntled employees can also deliberately destroy personal information. Also, changes to IT systems without proper IT change management process and lack of disaster recovery strategy could lead to loss of information.

Risk 6
E.g., The town loses control of electronic and/or paper-based information as a result of insufficient or absence of contractual agreements with a third-party service provider. Loss of custody may involve the theft of paper records or a server that contains personal information in the Town's premises.

Risk 7

E.g., information collected for this project is inadvertently or maliciously destroyed contrary to POPA and the policies of the Town, such that the Town is unable to respond to access to information requests or carry out its business functions. Lack of an enforceable record retention and disposition policy could also lead to unauthorized destruction.

Risk 8

E.g., information collected for this project is rendered inaccurate, or incomplete, contrary to section 6(a) of POPA. This may occur if employees are not adequately trained on good data entry practices or if system changes do not follow industry standard change management processes or information is not reasonably protected from unauthorized modification.

Risk 9

E.g., personal information collected for this project is retained contrary to section 6(b) of POPA or the project retention procedures as established by the public body (section 7(2)(f) of the M-Regulation). In some cases, this may be a consequence of the absence of a record retention policy or lack of enforcement of an existing record retention policy.

Risk 10

E.g., individuals' information is collected for this project without providing proper notice at the time of collection, contrary to section 5(2) of POPA. Notice fails to align with the manner of collection and the requirement of POPA such as collecting personal information directly from individuals by telephone but providing notice via the Town's website.

Risk 11

E.g., the Town fails to make individuals aware of their rights to request access to or correction of their personal information, and how to make such requests.

Risk 12

E.g., lack of or inadequate privacy breach management means that privacy breaches will not be consistently detected and managed. In addition, affected individuals of privacy breaches/incidents, the Commissioner and the Minister will not be notified in a timely manner as required under section 10(2) of POPA.

Risk 13

E.g. without assessing third parties' controls, the Town is unable to attest whether the third party reasonably protects personal information in respect of the services provided to the Town in compliance with POPA and its regulations. As a result, the Town could fail to meet its obligations to protect personal information under section 10 of POPA.

Risk 14

E.g. personal information collected for this project for purposes under section 12 of POPA is being used for secondary purposes (e.g. to train artificial intelligence (AI) or by the third party for quality improvement purposes) without authority.

Risk 15
E.g., inadequate or absence of logging capabilities of systems limits the ability of the Town to identify and manage privacy breaches of personal information. In addition, it limits the Commissioner's ability to investigate access to personal information violations including investigating potential offences under section 60 of POPA.

Risk 16
E.g., failure to have human oversight and validation measures for information systems could potentially lead to data accuracy and reliability issues.

Risk 17
Failing to conduct a security vulnerability assessment means that the Town may not be aware of exploitable security vulnerabilities that exists in its environment and as a result, would not take steps to address those security vulnerabilities in a timely manner thereby exposing personal information to potential compromise.

H2. Risks Associated with Cloud Computing

Risk 1
E.g. In a multitenant cloud environment, compromise of one environment could lead to the compromise of other environments due to inappropriate segregation and isolation of cloud resources. In addition, there could potentially be information leakage between environments leading to unauthorized disclosure of personal information.

Risk 2
E.g., lack of formalized contractual arrangements that specifically consider POPA requirements could lead to loss of custody and/or control of personal information stored in the cloud environment as well as gaps in security management and non-compliance with POPA.

Risk 3
E.g. the absence of clear and good governance on privacy and security of personal information could result in gaps in privacy and security management leading to non-compliance with POPA.

Risk 4
E.g., POPA requirements including privacy breach management is not addressed in the contractual agreement between the public body and the cloud provider, which could lead to non-compliance with section 10(2) of POPA.

Risk 5
E.g. a cloud provider goes out of business or declares bankruptcy, making it impossible for the public body to access personal information in the provider's environment.

Risk 6
E.g., a cloud provider uses proprietary technologies, making it difficult for the Town to migrate services to another provider, locking-in the Town. The Town may want to change provider if the existing provider suffers multiple security incidents that have caused privacy breaches.

Risk 7
E.g., the USA PATRIOT Act and Cloud Act allow the US government to access personal information held by US-based companies in the US (USA PATRIOT Act) and anywhere in the world (Cloud Act).

Risk 8
E.g., a cloud provider uses personal information for their own purposes, such as de-identifying personal information and/or using the personal information for training their AI models.

Risk 9
E.g., the cloud provider sells personal information or fails to securely sanitize information processing media prior to re-use or disposition leading to unauthorized disclosure of the personal information.

Risk 10
E.g. lack of reasonable authentication and authorization controls such as failures to implement and enforce multifactor authentication could potentially lead to unauthorized access to personal information.

Risk 11
E.g. weak or lack of encryption could lead to unauthorized access to and disclosure of personal information in transit and at rest.

H3. Risks Associated with Research

Risk 1
E.g., the Town fails to assess whether non-identifying data can be used to accomplish the research purpose prior to disclosing individually identifying personal information or has not obtained the Commissioner's approval for such disclosure as required under section 15(a) of POPA.

Risk 2
E.g., the Town fails to perform a public interest analysis prior to disclosing personal information for research or statistical purposes where the information is involved in data matching.

Risk 3
E.g. the Town fails to conduct an assessment of risk of harm prior to disclosing personal information for research or statistical purposes where the information is involved in data matching.

Risk 4
E.g., the Town has not approved conditions relating to security and confidentiality, the removal or destruction of individual identifiers and prohibition of subsequent use or disclosure of the information without express authorization of the Town.

Risk 5
E.g., a research agreement has not been signed prior to the Town disclosing personal

information or the research agreement in place does not meet the requirements of section 15(d) of POPA and section 4 of the Regulation.

Appendix A. Data Matching

Only complete this section if the project involves data matching as defined under section 1(f) of POPA.

Question 1
No additional explanation needed.

Question 2
There are specific circumstances in which the Town may *c*arry out data matching as listed in section 17(1) of POPA. Any prescribed purposes will be found in the regulation otherwise such a purpose does not exist.

Question 3
No additional explanation needed.

Question 4
Prior to collecting personal information from another public body for the purpose of data matching, the Town must first create a governance structure that clearly identifies the responsibilities and accountability of each public body involved in carrying out the data matching to ensure access and privacy rights of Albertans are protected. The governance structure must clearly identify the responsibilities and accountability of each public body as it relates to:

1. the custody and control of personal information,
2. the correction of errors or omissions in an individual's personal information,
3. breach notifications, and
4. other duties imposed by the Act.

The Town must meet this requirement before submitting their PIAs to the Commissioner for review.

Question 5 – The data matching agreement is required to ensure clarity regarding the roles and responsibilities of each public body involved in the data matching project as well as legislative compliance. The minimum requirements of the agreement are as follows:

the agreement must:

1. identify

(i) the authority under which the public body will carry out data matching, and

(ii) the purpose for which the public body will carry out data matching,

1. identify each public body's role and how each public body's role relates to the purpose of the data matching to which the addendum relates,
2. describe how the personal information will be securely transmitted, matched or linked by the public bodies,
3. identify whether the data derived from the personal information used for data matching will be disclosed to the public body from whom the personal information was collected,
4. identify each public body's responsibilities respecting reasonable security arrangements, including respecting administrative safeguards, physical safeguards and technical safeguards, for the protection of personal information against such risks as unauthorized access, collection, use, disclosure or destruction, and
5. establish a clear governance structure respecting the responsibilities and accountability of each public body.

Question 6

This question requires that a public body participating in data matching identifies collections, uses or disclosures of personal information that only apply to that public body. In doing so, the public body is required, by law, to have an addendum for the unique collections, uses or disclosures to accompany the join PIA submitted for the project.

Question 7

No additional explanation needed.

Question 8

Risk Assessment and Mitigation – Risks Associated with Data Matching.

This Completion Guide will provide some examples of the description of the types of risks identified in the Risk Assessment and Mitigation table for risks related to data matching.

Risk 1

E.g. section 7(2)(g) of the M-Regulation requires the establishment of a clear governance structure respecting the responsibilities and accountability of two public bodies involved in data matching if one public body is collecting personal information from another public body for the purpose of data matching.

Risk 2

E.g., this risk assessment is to ensure that section 17 of POPA is complied with, given that this section prohibits public bodies, except for the Office of Statistics and Information, from collecting personal information directly from an individual for the purpose of data matching.

Risk 3

E.g., section 6 of POPA requires the Town to make every reasonable effort to ensure that an individual's personal information is accurate and complete before using such information to make a decision that directly affects that individual.

Risk 4

E.g., as required by section 6 of POPA, the quality of the source data will play a significant part in the quality of the resulting data from data matching, so it is important for the Town to ensure that the quality of the source is validated prior to conducting the data matching.

Risk 5

E.g., data matching activities normally take place in a test environment. The resulting data is then migrated to the production environment. Therefore, the test environment security controls should be proportionate to the security classification of the data involved in data matching. Failure to implement reasonable and proportionate security arrangements to protect personal information within the Town's data matching environment, exposes it to potential incidents under section 10 (2) of POPA especially given that a single test environment may be used for multiple projects and thus accessed by various users.

Risk 6

E.g. this is about validating the final product. The Town should ensure that the final product is the desired outcome, and that no data errors are in the resulting data set, or if errors are identified, that they are addressed. (section 6 of POPA).

Risk 7

E.g., this is about securely cleaning the test environment that was used for data matching by securely deleting personal information from that environment before it is used for other purposes or used by other users to prevent potential unauthorized access to personal information.

Appendix B. Common or Integrated Program or Service

Question 1

A common or integrated program or service must comply with specific requirements under POPA and the M-Regulation. It is therefore important for the Town to carefully consider those requirements prior to implementing new common or integrated program or service or making changes to an existing common or integrated program or service.

Question 2

Since common or integrated program or services requires each public body to identify its responsibilities and accountabilities identifying each public body assist in determining the areas of responsibility and accountability for each public body.

For question 2c, if the PIA is for a change in an existing common or integrated program or service, providing an existing PIA file number assists the OIPC in making reference to relevant information in that file during the review of the current PIA as the Town focuses on addressing privacy and security risks associated with the change. The Town may also choose to use the existing Microsoft Word copy of the existing PIA to identify areas that have changed by striking the outdated information and entering updated or new information in a different-colour text.

Question 3

This question is about making sure that there is a governance structure in place for the common or integrated program or services. This governance structure *(a documented set of rules and processes that identify the roles, responsibilities and accountability for each public body participating in the integrated program or service),* that clearly identifies responsibilities and accountabilities must be in place prior to the PIA being submitted to the Commissioner for review.

The governance structure must clearly identify the responsibilities and accountability of each public body as it relates to:

1. the custody and control of personal information,
2. the correction of errors or omissions in an individual's personal information,
3. breach notifications, and
4. other duties imposed by the Act.

Question 4

This agreement is required to ensure each public body involved in a common or integrated program or service independently comply with POPA**.** The minimum requirements for such an agreement include:

1. identify the purpose of the common or integrated program or service,
2. identify each public body's roles and responsibilities respecting the common or integrated program or service and how the roles and responsibilities of each public body relate to the purpose of the common or integrated program or service, identify each public body's responsibilities under the Act,
3. establish rules respecting reasonable security arrangements, including respecting administrative safeguards, physical safeguards and technical safeguards, for the protection of personal information against such risks as unauthorized access, collection, use, disclosure or destruction, and

4. establish a clear governance structure respecting the responsibilities and accountability of each public body.

Question 5

This question requires that a public body participating in a common or integrated program or service identifies collections, uses or disclosures of personal information that only apply to that public body. In doing so, the public body is required, by law, to have an addendum PIA for the unique collections, uses or disclosures to accompany the joint PIA submitted for the project.

Question 6

Risk Assessment and Mitigation – Common or Integrated Program or Service Risks

This completion guide will provide some examples of the description of the types of risks identified in the Risk Assessment and Mitigation table for common or integrated program or service risks

Risk 1
E.g., governance structure including policies are not in place or are inadequate leading to inconsistencies in the management of the program that creates exploitable privacy and security vulnerabilities.

Risk 2
E.g., policies are not in place or are not clear on accountability for different aspects of the program including accountability for privacy.

Risk 3

E.g., the responsibilities of each public body involved in the common or integrated program including for privacy management are not clearly defined.

Risk 4

E.g., the information security classification for one or more public bodies do not align with the sensitivity of information, leading to gaps in the protection of personal information.

Risk 5
E.g., the public bodies involved fail to make individuals aware of how they can exercise their access and privacy rights under applicable POPA and ATIA.

Appendix C. Use of Automated Systems or Other Forms of Innovative Technology

Question 1

An Algorithm Impact Assessment (AIA), is a risk assessment or evaluation process that determines the impact of an automated system on individuals whose personal information is collected, used or disclosed in the use of automated systems such as artificial intelligence or other forms of innovative technology. Section 7(3) of the M-Regulation requires that a PIA contains a level of detail commensurate with the complexity of the practice, program, project or service the PIA relates to. As such, the Town is required to also complete an AIA. The OIPC is in the process of developing an AIA tool, which will be published on the OIPC website and a link included in the POPA PIA template and this document. In the interim, the OIPC recommends that where a project involves automated systems, the Town consult industry standard algorithm impact assessment guidelines in preparing and submitting their AIAs with their PIAs.

Question 2

Risks Associated with the use of Automated Systems or other forms of innovative technology.

Risk 1
E.g. failure to maintain custody or control of personal information ingested by an automated system due to lack of controls to securely and automatically delete information from the automated system.

Risk 2
E.g. lack of or insufficient automated systems governance policies and procedures leads to inconsistent implementation and use of automated systems, resulting in automated systems-related vulnerabilities and privacy compliance issues.

Risk 3
E.g. automated systems such as artificial intelligence, are known to hallucinate by fabricating results or outputs. Lack of monitoring including lack of oversight of AI systems leads to failures to detect and address hallucination issues.

Risk 4
E.g. Using poor quality and unreliable training data leads to issues with automated systems results including hallucination. In addition, using training data that is not an accurate representation of the population where the automated systems will be deployed could potentially lead to inaccurate results and bias.

Risk 5
E.g. if inputs in automated systems are not validated and protected, such inputs can be manipulated prior to processing by the automated system. This makes input vulnerable to tampering and the automated system vulnerable to faulty results.

Risk 6
E.g., understanding whether the automated system model is static or dynamic, it may be difficult to implement the right monitoring mechanism for the models. For instance, while

dynamic models continuously learn from new data sets in process, a static model is as good as its last update.

Risk 7
E.g., Underfitting an automated system model with its training data means that the automated system model is trained to be too broad in its generalization making the model prone to false positives when processing new data.

Risk 8
E.g., Overfitting an automated system model with its training data means that the automated system model is trained too closely aligned with its training data, leading to lack of generalization by the model and making the model prone to false negatives when it processes new data.

Risk 9
E.g., misconfiguration of an automated system is a security vulnerability that could be exploitable, leading potential to unauthorized access to or disclosure of personal information.

Risk 10
E.g., lack of processes for individuals to be made aware of and appeal decisions made by automated systems could infringe on individuals' access and privacy rights.

Risk 11 – E.g., insufficient logging and auditing means that the activities of the automated system cannot be reasonably monitored to ensure it is working as expected or to detect potential compromise of the system.

Risk 12
E.g., lack of monitoring of the automated system based on established policies and processes means that issues with the functioning of the automated system cannot be detected and addressed in a timely manner.

Risk 13
E.g., without conducting a vulnerability assessment means that exploitable vulnerabilities associated with an automated system cannot be identified and addressed. A copy of the results of the assessment should form part of the PIA to demonstrate the Town's commitment to protect personal information pursuant to section 10 of POPA.

Appendix D. PIA Cover Letter *

While the head of the Town may assign privacy responsibilities to other individuals within the Town, the head of the Town is ultimately accountable for meeting the Town's obligations under POPA. To this end, the PIA must include a cover letter signed by the head of the Town.

Appendix E. PIA Submission Checklist *

This checklist is there to ensure the Town reviews its PIA and ensures all sections of the PIA have been considered, relevant sections completed, and all supporting document included in the PIA submission.

Schedule "K"

PERSONAL INFORMATION BANK

DIRECTORY OF PERSONAL INFORMATION BANK

Strathmore
Rural Reimagined

Compiled by: Legislative Services – ATI Coordinator

Updated as of March 2026

TABLE OF CONTENTS

Introduction

Purpose of the Protection of Privacy Act (POPA)

Impact of the Act

Purpose of the Access to Information Act (ATIA)

Impact of the Act

Privacy and ATI Contacts

Privacy Officer

Privacy Head

ATI Coordinator

ATI Head

Directory of Terms

Exceptions to Disclosure

ATIA and POPA Head/ATI Coordinator and POPA Officer

Personal Information Bank

Personal Information

Record

Directorates

CAO Office

Human Resources

Economic Development

Community & Protective Services, Recreation and Culture

Strathmore Fire Department

Municipal Enforcement

Recreation (Aquatic Centre, Family/Civic Centre, and Sports Centre)

Infrastructure, Operations, and Development Services

Infrastructure

Operations

Planning & Development

Strategic, Administrative & Financial Services

Legislative Services

Marketing & Communications

Finance (Admin, Assessment & Taxation, Finance, and Utilities)

Information Technology

Special Events Coordinator

Legal and Risk Management

INTRODUCTION

Alberta has modernized its access to information legislation. The *Protection of Privacy Act*, often referred to as POPA, and the *Access to Information Act,* often referred to ATIA, came into force on June 11, 2025, and replaces the *Freedom of Information and Protection of Privacy Act*.

POPA is the legislative framework by which public bodies may collect, use, or disclose personal information and requires the protection of personal information held by public bodies. The POPA Act also permits public bodies to collect, use or disclose personal information in new ways, including for data matching and to create non-personal data.

The *Access to Information Act* allows access to records held by public bodies in Alberta and is the cornerstone of an open, accessible and accountable public body. It aims to strike a balance between the public's right to know information and protecting confidential information required to ensure effective operations of government and public bodies.

Purpose of the Protection of Privacy Act

The *Protection of Privacy Act* replaced the privacy part of is the *Freedom of Information and Protection of Privacy Act*. The purposes of the Act are to control the collection, use and disclosure of personal information by a public body, to allow individuals a right to request corrections to personal information about themselves that is held by a public body, to control the creation, use and disclosure of data derived from personal information and non-personal data by a public body, and to provide for independent reviews of decisions made by public bodies under this Act and the resolution of complaints under this Act.

Impact of the Act

POPA has provisions concerning when public bodies must submit privacy impact assessments to the Commissioner, requirements concerning privacy management programs (the requirements related to privacy management programs will apply as of June 11, 2026), and privacy breach notification requirements when an incident involving the loss of or unauthorized access to or disclosure of personal information could result in a real risk of significant harm to individuals.

Individuals have rights under POPA as it relates to their personal information including:

- the right to ask a public body to correct their personal information,
- the ability to make a complaint if they believe that their personal information is being collected, used or disclosed contrary to the Act.
- The Act also allows individuals to make a complaint to the Commissioner about data derived from personal information or non-personal data that has been created, used or disclosed in contravention of the Act or respecting the actual or attempted re-identification of non-personal data created under the Act.

Purpose of the Access to Information Act

The purposes of this Act are to allow any person a right of access to the records in the custody or control of a public body subject to limited and specific exceptions as set out in this Act, to allow individuals, subject to limited and specific exceptions as set out in this Act, a right of access to personal information about themselves that is held by a public body, and to provide for independent reviews of decisions made by public bodies under this Act and the resolution of complaints under this Act.

Impact of the Act

ATIA establishes rights for persons to access records, as defined in the ATIA, that are in the custody or control of public bodies subject to limited and specific exceptions.

The *Protection of Privacy Act* and the *Access to Information Act* will hold the Town of Strathmore accountable for its records and information management practices concerning access to information and privacy protection to an external authority, the Information and Privacy Commissioner.

The Directory of Personal Information Banks is intended for use of the POPA Head, POPA Officer, ATI Head, ATI Coordinator, Town of Strathmore staff within all departments and members of the public as a method of determining the location of the Town of Strathmore records within various departments. The Town of Strathmore recommends that any inquiries about a record be directed to the department that has custody or control of the record. Formal written requests for information under the POPA and ATIA are to

be directed to the ATI Coordinator, Town of Strathmore at 1 Parklane Drive, Strathmore, Alberta, T1P 1K2 or by calling 1-403-934-3133 or by emailing ATIA@Strathmore.ca.

The *Protection of Privacy Act* and the *Access to Information Act* will hold the Town of Strathmore accountable for its records and information management practices concerning access to information and privacy protection to an external authority, the Information and Privacy Commissioner.

The Directory of Personal Information Banks is intended for use of the POPA Head, POPA Officer, ATI Head, ATI Coordinator, Town of Strathmore staff within all departments and members of the public as a method of determining the location of the Town of Strathmore records within various departments. The Town of Strathmore recommends that any inquiries about a record be directed to the department that has custody or control of

the record. Formal written requests for information under the POPA and ATIA are to be directed to the ATI Coordinator, Town of Strathmore at 1 Parklane Drive, Strathmore, Alberta, T1P 1K2 or by calling 1-403-934-3133 or by emailing ATIA@Strathmore.ca.

Note: Personal information collected by the Town of Strathmore may be disclosed in accordance with the Act.

FOIP CONTACTS

CONTACT	TELEPHONE	EMAIL
POPA Officer / ATI Coordinator		
Ms. Claudette Thorhaug 1 Parklane Dr Strathmore, AB T1P 1K2	1-403-934-3133	ATIA@Strathmore.ca
POPA Head / ATI HEAD		
Ms. Kara Rusk 1 Parklane Dr Strathmore, AB T1P 1K2	1-403-934-3133	ATIA@Strathmore.ca

DIRECTORY OF TERMS

Exceptions to Disclosure Exceptions to disclosure are a provision of the Act, which either require or permit refusal of the right of access to records or personal information in the custody or under the control of the Town of Strathmore. The Act specifies limited and specific exceptions where disclosure would result in harm to government or a third party. These exceptions are set out in Sections 19 to Section 34

ATI Head / Coordinator An employee of the Town of Strathmore delegated the responsibility of processing Access to Information requests.

Personal Information Bank A collection of personal information that is organized or retrievable by the name of the individual or by an identifying number, symbol or other assigned to an individual.

Personal Information Personal information means recorded information about an identifiable individual, including:

- the individual's name, home or business address or home or business telephone number, home or business email address or other contact information, except where the individual has provided the information on behalf of the individual's employer or principal, in the individual's capacity as an employee or agent,
- the individual's race, national or ethic origin, colour or religious or political beliefs or associations,
- the individual's age, gender identity, sex, sexual orientation, marital status, or family status,
- an identifying number, symbol, or other particular assigned to the individual,
- the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,
- information about the individual's health and health care history, including information about the individual's physical or mental health,
- information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,
- anyone else's opinions about the individual, and
- the individual's personal views or opinions, except if they are about someone else.

Record	A record means any electronic record or other record in any form in which information is contained or stored, including information in any written, graphic, electronic, digital, photographic, audio or other medium, but does not include any software or other mechanism used to store or produce the record.

General

Title	**Outlook - Contacts**
Location	Various departments of the public body
Information	Name, address, telephone number and email address
Individuals	Personal and Business Contacts, Staff Members
Use	Contacts and daily business within the Town of Strathmore
Legal Authority	Section 4(c) of the Protection of Privacy Act

Title	**M-Files**
Location	Various departments of the public body
Information	Name, address, telephone number and email address
Individuals	Town administrative processes
Use	Document/Records Management
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**CorePoint**
Location	HR Department Software
Information	Username, User Address, User Employee Number, User Emergency Contacts (Name, Address, Phone Number), User Birthday
Individuals	Town OH&S processes
Use	Documentation

Legal Authority	Section 4(c) of the *Protection of Privacy Act, OH&S Act*

CAO OFFICE - Human Resources and OH&S

Title	**Employee Database/ HR Files**
Location	Human Resource Department – GP (Payroll/HR) and Employee Files (Locked Storage and Secure HR M-Files vault)
Information	Employee name, employee number, mailing address, telephone number, date of birth, social insurance number; performance reviews; training session history information; employee history and years of service; retirement / LAPP service; salary and vacation entitlement information; driver's abstract (if required); criminal record history; employee emergency contact information, next of kin; dependent names and date of birth for each child; registered retirement savings plan information; HR Forms
Individuals	Employees of the Town
Use	Record keeping of current and former employees to administer health benefits, salary increments, pension program and RRSP contributions
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Employee Competition Files**
Location	Human Resource Department – Public Drive (Permissions in place)
Information	Applicant's name, address, telephone number, email address; resume, reference name, address, telephone number; interview notes; questions and answers; reference information collected and driver's abstract
Individuals	Individuals who have applied for or interviewed for a position at the Town
Use	To find suitable candidates for various positions with the Town of Strathmore
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Exit Interview Notes**
Location	Human Resource Department
Information	Interviewee name
Individuals	Staff who have had an exit interview with the Town
Use	To gather exiting employee's feedback as part of the Human Resource program
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Payroll Database (GP)**
Location	Human Resource Department
Information	Employee name, employee ID, address, telephone number, date of birth, social insurance number; current and historical salary; rate of pay; benefits; exception reporting and time entry; earnings and deductions; banking information; email address; tax information; LAPP; WCB
Individuals	Employees on Town payroll
Use	Administration of the Town's payroll program
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Payroll Updates - WCB Database**
Location	Human Resource Department
Information	Name, department, status, coding, continue benefits/pension while off
Individuals	Individuals on WCB compensation
Use	To administer the Health and Safety program, provide payroll with coding and hours for people on WCB claims per pay period
Legal Authority	*Occupational Health and Safety* Act and Section 4(c) of the *Protection of Privacy Act*

Title	**Workers Compensation Board Claim Forms (Employer's Report)**
Location	Human Resource Department (CorePoint & M-Files)
Information	Claim number and type; name, address, telephone number, email address, social insurance number, Alberta Health Care number, date of birth, gender; employer information including Worker's Compensation Board (WCB) account number; date and time of injury; name and telephone number of the person notified of the injury; description of what occurred to cause the injury; time lost and return to work information including pre-accident rate of pay; wage information including date of hire; rate of pay at the time of the accident; earnings information contact name and telephone number
Individuals	Individuals who have been injured at work and persons notified of the injury
Use	To determine entitlement to compensation and for determining employers' premium rates
Legal Authority	*Workers' Compensation Act* and Section 4(c) of the *Protection of Privacy Act*

Title	**Workers Compensation Board Forms (Worker Physical Demands Analysis)**
Location	Human Resource Department (CorePoint)
Information	Claim number; employee name; employer contact information, telephone number and activity to be undertaken
Individuals	Individuals who have been injured at work
Use	To determine entitlement to compensation and for determining employer premiums
Legal Authority	*Workers'* Compensation Act; and Section 4(c) of the *Protection of Privacy Act*

Title	**Workers Compensation Board Tracking Database**
Location	Human Resource Department
Information	Name; department; type of injury; month of injury; lost time days; whether claim was accepted or not; Leave tracking for short/long term WCB
Individuals	Individuals who have been injured at work

Use	To determine entitlement to compensation and for determining employers' premium rates
Legal Authority	Section 4(c) of the *Protection of Privacy Act*
Title	**Incident Reporting**
Location	Human Resource Department (CorePoint)
Information	Date, time and location of the incident; name of person and department the incident was reported by; name of the person who the incident was reported to; name, address, telephone number of person involved in the incident including witnesses and property owner name; conditions and description at the time of the incident; driver history information (if applicable) including name, driver's license number, particulars of injured person including name, address and telephone number; name of person who administered first aid; name of person who transported the injured to medical aid; name of person investigating the incident; name of person responsible for implementing actions
Individuals	Individuals involved in an incident, individuals assisting or transporting an injured person, individuals reporting or investigating incident, individuals responsible for implementing actions, individuals identified on the incident report form
Use	Administration of the Town of Strathmore's Health and Safety Program
Legal Authority	*Occupational Health and Safety Act* and Section 4(c) of the *Protection of Privacy Act*
Title	**Compensation Board Claim Forms (Worker's Report)**
Location	Human Resource Department (CorePoint)
Information	Claim number; name, address, telephone number, email address, social insurance number, Alberta Health Care number, date of birth, gender of injured employee; date and time of injury; name and telephone number of the person notified of the injury; description of what occurred to cause the injury; list of persons who witnessed the accident; return to work information including pre-accident rate of pay; wage information including date of hire;

	rate of pay at the time of the accident
Individuals	Individuals who have been injured, individuals notified of the injury, individuals who witnessed accident
Use	To determine entitlement to compensation and for determining employers' premium rates
Legal Authority	*Workers' Compensation Act*; and Section 4(c) of the *Protection of Privacy Act*

Title	**Safety Training Matrix Database**
Location	Human Resource Department (CorePoint)
Information	Name, job title, employee number, department, status, hire date, orientation date and courses taken, date and expiry dates
Individuals	Individuals who enroll in employee training
Use	Administration of the Health and Safety program, record keeping of required and taken employee training
Legal Authority	*Occupational Health and Safety* Act and Section 4(c) of the *Protection of Privacy Act*

Title	**Audiometric Testing Database**
Location	Human Resource Department (CorePoint)
Information	Name, department, status, audio testing historical dates and required dates Individuals
Use	To administer the Health and Safety program, record audiometric testing dates and ensure recall at required intervals
Legal Authority	*Occupational Health and Safety Act* and Section 4(c) of the *Protection of Privacy Act*

CPS – FCSS

Title	**FCSS Forms**
Location	FCSS Department

Information	Name, Address, Phone, Birthdate, SIN #, Income, Emergency Contact & Phone number, and Credit Card #
Individuals	Individuals who participate in FCSS Programs
Use	Management of the following FCSS Programs – Community Access, Income Tax, Good Food Box, Frozen Meals, FCSS Intake, Seniors Tax, Kare Driver, Delivery Contract, Tools for School, Intake Information
Legal Authority	Section 4(c) of the Protection of Privacy Act

Title	**FCSS Forms sent to the Government**
Location	FCSS Department
Information	Name, Address, Phone, Birthdate, SIN #, Income, Emergency Contact & Phone number, and Credit Card #
Individuals	Individuals who participate in FCSS Programs
Use	Forms sent to the Government - Aish Forms, CPP, OAS, GIS, Alberta Supports, Alberta Senior Benefits, Adult Health Benefits and Child Health Benefits
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

CPS - Strathmore Fire Department

Title	**Fire Pro Software**
Location	Strathmore Fire Department
Information	Incident number; location of incident, description of incident and actions taken; type of call; name, address and telephone number of owner; name, address and telephone number of occupant; make, model, year of vehicle; insurance company and policy number; driver's license number; incident commander's name; Motor Vehicle Crash Information: driver name, address, driver's license number; insurance company name, agent's name, telephone number, insurance policy number; RCMP detachment member file number; vehicle identification number

Individuals	Individuals involved in or witness to an incident
Use	Used for billing purposes, Incident Documentation, Provincial Reporting, Investigations
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Alberta Infrastructure (Fire call and Rescue Information)**
Location	Strathmore Fire Department
Information	Date of service; call type; incident number; location of incident; name of attendant; name, address, telephone number (home and business) of driver/owner; registered owner/insurance company agent name and policy number
Individuals	Driver or registered owner involved in incident, insurance agents
Use	Town of Strathmore for billing purposes.
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Fire Database**
Location	Strathmore Fire Department
Information	Name, mailing address, legal land description, inspection date, incident date, list of building fire code deficiencies, insurance information
Individuals	Owner, occupant, management company representatives or insurance agents
Use	Administration related to Fire Inspection Records, Burn Permits, Fire Investigation Reports
Legal Authority	*Safety Codes Act*, 26(1), 31(1), 34 35, 48; Administrative Items Regulations (A.R. 16/2004) s. 9; *Municipal Government Act*; Section 4(c) of the *Protection of Privacy Act*; Strathmore Fire Department Level of Service Policy

Title	**Applications – Fire Works**
Location	Strathmore Fire Department
Information	Name, Address, Certification, copy of Driver Licenses, Insurance

Individuals	Applicants for Fire Works
Use	Used for permit process
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Voyent Alert**
Location	Strathmore Fire Department – Voyent Software
Information	Name, Address, Email, telephone number
Individuals	Individuals that sign up for the alert system
Use	Administration of the Voyent Alert System
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

CPS – Municipal Enforcement

Title	**Voluntary Payment Ticket – Dog/Cat Control**
Location	Municipal Enforcement
Information	File & ticket number, penalty; summons information, offence date and time, dog license number, owner's name, address, date of birth, issuer's signature, and badge number
Individuals	Individuals who have been issued a ticket under bylaw, ticket issuer
Use	To process infractions under bylaw
Legal Authority	Bylaw No. 22-20 and Section 4(c) of the *Protection of Privacy Act*

Title	**Violation Tag – Dog/Cat Control**
Location	Municipal Enforcement
Information	File & ticket number, penalty; summons information, offence date and time, dog license number, owner's name, address, date of birth, issuer's signature, and badge number

Individuals	Individuals who have been issued a ticket under bylaw, ticket issuer
Use	To process infractions under bylaw
Legal Authority	Bylaw No. 22-20 and Section 4(c) of the *Protection of Privacy Act*

Title	**Urban Hen Application Form**
Location	Municipal Enforcement
Information	Name of applicant, address, contact number, Name, phone number, and address of a temporary hen keeper, hen course certificate
Individuals	Individuals who have been issued a ticket under bylaw, ticket issuer
Use	To process infractions under bylaw
Legal Authority	Bylaw No. 22-06 and Section 4(c) of the *Protection of Privacy Act*

Title	**Violation Tag – Traffic**
Location	Municipal Enforcement
Information	File & ticket number, penalty; summons information, offence date and time; description of vehicle; license plate or VIN #, issuer's signature and badge number
Individuals	Individuals who have been issued a ticket under bylaw, or applicable provincial legislation, ticket issuer
Use	To process infractions under bylaw
Legal Authority	Bylaw No. 22-06 and Section 4(c) of the *Protection of Privacy Act*

Title	**Voluntary Payment Ticket – Traffic**
Location	Municipal Enforcement
Information	File & ticket number, penalty; summons information, offence date and time; description of vehicle; license plate or VIN #, registered owner's name, address, date of birth and driver's license number & MVID; issuer's signature and badge number

Individuals	Individuals who have been issued a ticket under bylaw, ticket issuer
Use	To process infractions under bylaw
Legal Authority	Bylaw No. 22-06, *Traffic Safety Act* and Section 4(c) of the *Protection of Privacy Act*

Title	**Voluntary Payment Ticket – Traffic**
Location	Municipal Enforcement
Information	File & ticket number, penalty; summons information, offence date and time; description of vehicle; license plate or VIN #, registered owner's name, address, date of birth and driver's license number & MVID; issuer's signature and badge number
Individuals	Individuals who have been issued a ticket under bylaw, ticket issuer
Use	To process infractions under bylaw
Legal Authority	Bylaw No. 22-06, *Traffic Safety Act* and Section 4(c) of the *Protection of Privacy Act*

Title	**Disbursement Report**
Location	Municipal Enforcement
Information	Name and address of accused; amount of the violation ticket and whether the penalty has been paid
Individuals	Individuals issued a violation ticket
Use	Used by administrative staff to track violation ticket status
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Outstanding Warrant Forms**
Location	Municipal Enforcement
Information	Name, date of birth and last known address of accused, ticket number
Individuals	Individuals issued an outstanding warrant
Use	Used by administrative staff to track violation ticket status

Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Alberta Justice Report**
Location	Municipal Enforcement
Information	Name of accused; docket number; action taken and charges
Individuals	Individuals issued a violation ticket and appearing before Alberta Justice
Use	Used by Alberta Justice staff at Court House and status of tickets
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Notice of Vehicle Seizure**
Location	Municipal Enforcement
Information	Name, gender, date of birth, operator's license number, address, telephone number and vehicle identification number (VIN) of driver; name, gender, date of birth, operator's license number, address, telephone number and VIN of registered owner (if different from the driver's information); vehicle information including license plate number, province of issue, VIN, year, make and model; reason for seizure, immobilization or removal; company name, address and telephone number of vehicle impoundment area; name of towing company and signature of representative; police file number; regimental number
Individuals	Drivers, owners, insurers, towing company representatives
Use	To track seized vehicles by administrative staff and officers
Legal Authority	*Traffic Safety Act*, Bylaw No. 22-06, *Traffic Safety Act* and Section 4(c) of the *Protection of Privacy Act*

Title	**Prosecutor Information Sheet**
Location	Municipal Enforcement
Information	Investigator's name; accused name and address; offense, offence date and offence location, circumstances of the offence; and witness' name
Individuals	Investigators, accused individuals, witnesses

Use	A trial file for the Prosecutor
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Request for Justice of the Peace Services Fax Cover Sheet**
Location	Municipal Enforcement
Information	Police file number; Crown Prosecutor or Presiding Officer's name and telephone number; accused name
Individuals	Crown Prosecutors, Presiding Officers, accused individuals, fax operators
Use	To request Justice of the Peace Services from the Department of Alberta Justice
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Remedy Order Regarding Unsightly**
Location	Municipal Enforcement
Information	File number; name and address of registered owner; description of untidy and unsightly premises and signature of Community Peace Officer
Individuals	Property Owners, Peace Officers, Municipal Enforcement Officers
Use	To process a written Order under the Town of Strathmore's Unsightly Premises
Legal Authority	Community Standards Bylaw No. 13-05 and Section 4(c) of the *Protection of Privacy Act*

Title	**Notice to Owner Regarding Unsightly Premises (Community Standards Bylaw)**
Location	Municipal Enforcement
Information	File number; name and address of registered owner; description of untidy and unsightly premises and signature of Community Peace Officer
Individuals	Property owners, Peace Officers
Use	To provide written notice to a landowner regarding unsightly property
Legal Authority	Community Standards Bylaw No. 13-05 and Section 4(c) of the *Protection of Privacy Act*

Title	**Citizen Complaint Form**
Location	Municipal Enforcement - Report Exec., Municipal Enforcement Inbox
Information	Description of the complain, photos, supporting documents narrative, location of incident, full name, address, telephone number
Individuals	Accused individuals, family of accused, pet owners, complainants, family of complainants, registered owners, vehicle owners, drivers, business owners, renters, witnesses, residents within Strathmore
Use	To process resident's concerns and any infractions of Town of Strathmore bylaws, Provincial Acts or Regulations.
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

CPS – Recreation

Title	**Recreation Management System – PerfectMind**
Location	Aquatic Centre, Civic Centre, Family Centre, Sports Centre, and Community Events
Information	Name, phone number, age, birthdate, address, email address, gender, picture, emergency contact, payment information, and registration history
Individuals	Individuals who have done the following recreation-related activities: applied for a recreational pass; registered for a program; bought products or services; booked a facility; used online services for customers. Vendor events for Economic Development.
Use	Administration of recreation-related activities and events, rental agreement, and waiver forms
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Summer Camp Registration Package**
Location	Summer Camp Folder – TOS Public Drive
Information	Participant information, caregiver information, emergency contact information, health history & medical

	information, media consent form, Participant risk acknowledgement & waiver.
Individuals	Summer camp participants
Use	The information is used to ensure the safety of our summer camp participants, and program liability release.
Legal Authority	*Municipal Government Act*

Title	**Summer Camp Participant Sign-in/Sign-out Sheet**
Location	Summer Camp Folder – TOS Public Drive
Information	Participant's name, sign-in time, signature, sign-out time, and notes section.
Individuals	Summer camp participants
Use	The information is used to record summer camp attendance and participant pick-up.
Legal Authority	*Municipal Government Act*

Title	**Summer Camp Medical Dispensing Form**
Location	Summer Camp Folder – TOS Public Drive
Information	Name of child, purpose of medication, medication name, date prescribed, time of last dose, times to administer medication, dosage.
Individuals	Summer camp participants
Use	Consent and release for camp staff to be able to administer/hemp children take any required medication needed throughout the day.
Legal Authority	*Municipal Government Act*

Title	**Summer Camp Walk Home Form**
Location	Summer Camp Folder – TOS Public Drive
Information	Parent's name(s), & child(ren's) name(s).

Individuals	Summer camp participants
Use	The information is used to gather consent and permission to allow summer camp participants to walk home from camp on their own.
Legal Authority	*Municipal Government Act*

IODS – Planning and Development

Title	**Building Permit Application**
Location	Development Services Offices and Contractor Park Enterprises Ltd.
Information	Name, signature, property address, telephone number, legal description, permit number, name and address of sub-contractors used, credit card information for payment of permits, construction value, email address
Individuals	Property owners, applicants, contractors
Use	Administration of Building Inspections Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Energy Performance Compliance Checklist for Building Permit Applications with NBC 2019-AE**
Location	Development Services Offices and Contractor Park Enterprises Ltd.
Information	Name, signature, property address, telephone number, legal description, permit number, square footage, specifications of heating, water, and HVAC systems, wall and roof specifics, foundation, and basement information
Individuals	Property owners, applicants, contractors
Use	Administration of Building Inspections Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Hydronic Heating Specification Sheet**

Location	Development Services Offices and Contractor Park Enterprises Ltd.
Information	Name, signature, property address, telephone number, legal description, permit number, name and address of sub-contractors used, heating system specifications
Individuals	Property owners, applicants, contractors
Use	Administration of Building Inspections Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Fire Safety Plan Accompanying Building Permit Application**
Location	Development Services Offices and Contractor Park Enterprises Ltd.
Information	Name, signature, property address, telephone number, legal description, permit number, name and address of sub-contractors used, email address, project description
Individuals	Property owners, applicants, contractors
Use	Administration of Building Inspections Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Electrical Permit Application**
Location	Development Services Offices and Contractor Park Enterprises Ltd.
Information	Name, mailing address, signature, property address, telephone number, fax number, legal description, permit number, name and address of sub-contractors used, credit card information for payment of permits, construction value, email address, type of work
Individuals	Property owners, applicants, contractors
Use	Administration of Building Inspections Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Plumbing Permit Application**

Location	Development Services Offices and Contractor Park Enterprises Ltd.
Information	Name, mailing address, signature, property address, telephone number, fax number, legal description, permit number, name and address of sub-contractors used, credit card information for payment of permits, construction value, email address, type of work
Individuals	Property owners, applicants, contractors
Use	Administration of Building Inspections Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Gas Permit Application**
Location	Development Services Offices and Contractor Park Enterprises Ltd.
Information	Name, mailing address, signature, property address, telephone number, fax number, legal description, permit number, name and address of sub-contractors used, credit card information for payment of permits, construction value, email address, type of work
Individuals	Property owners, applicants, contractors
Use	Administration of Building Inspections Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Solid Fuel Burning Appliance Information Sheet**
Location	Development Services Offices and Contractor Park Enterprises Ltd.
Information	Name, property address, telephone number, legal description, permit number, name and address of sub-contractors used, email address, fax number
Individuals	Property owners, applicants, contractors
Use	Administration of Building Inspections Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Development Permit Application**

Location	Development Services Offices
Information	Name, signature, property address, telephone number, legal description, permit number, description of development, credit card information for payment of permits, land use district, email address, name and address of sub-contractors used
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act and the Municipal Government Act*

Title	**Development Permit Application Checklist Form**
Location	Development Services Offices
Information	Name, signature, name and address of sub-contractor, permit number, signature of sub-contractor
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act and the Municipal Government Act*

Title	**Development Permit Right of Entry & Owner Authorization Form**
Location	Development Services Offices
Information	Name, signature, property address, legal description, permit number, name and address of sub-contractors used
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act and the Municipal Government Act*

Title	**Development Permit Affidavit of Corporate Signing Authority Form**
Location	Development Services Offices
Information	Name, signature, name, and address of sub-contractors used, property address, legal description, permit number

Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Development Permit Public Amenities Disclosure and Tree Protection Plan Agreement Form**
Location	Development Services Offices
Information	Name, signature, name, and address of sub-contractors used, property address, legal description, permit number, phone number, email
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Development Permit Site Contamination Disclosure and Historical Site Remediation Form**
Location	Development Services Offices
Information	Name, signature, name, and address of sub-contractors used permit number
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Development Permit Secondary Suite Additional Checklist Form**
Location	Development Services Offices
Information	Name, signature, name, and address of sub-contractors used permit number
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program

Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Development Permit Sign Information Form**
Location	Development Services Offices
Information	Name, signature, name, and address of sub-contractors used permit number
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Temporary Outdoor Patio Pilot Project Form**
Location	Development Services Offices and Economic Development Offices
Information	Name, signature, phone number, email address, property address, name and address of sub-contractors used, permit number
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Water, Sanitary Sewer, and Storm Sewer Connection Permit**
Location	Development Services Offices and Contractor Park Enterprises Ltd (sometimes the application comes in with the Building Permit application)
Information	Name, signature, property address, telephone number, legal description, permit number, name and address of sub-contractors used, credit card information for payment of permits, picture of service connection, email address
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program

Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Municipal Right-of-way Works & Excavation Permit**
Location	Development Services Offices and Infrastructure Services Offices
Information	Name, signature, property address, telephone number, legal description, permit number, name and address of sub-contractors used, email address, fax number
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Municipal Right-of-way Works & Excavation Checklist**
Location	Development Services Offices and Infrastructure Services Offices
Information	Name, signature, permit number
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Business License Application Form**
Location	Development Services Offices and Economic Development Offices
Information	Name, signature, property address, telephone number, legal description, email address, fax number, provincial license or permit number if applicable
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program and Economic Development Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Land Use Bylaw Amendment Application Form**
Location	Development Services Offices and Legislative Services Offices
Information	Name, signature, property address, telephone number, legal description, permit number, description of development, land use district, email address
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Area Structure Plan Application Form**
Location	Development Services Offices and Legislative Services Offices
Information	Name, signature, property address, telephone number, legal description, permit number, description of development, email address, name and address of sub-contractors used
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Municipal Government Act*

Title	**Area Structure Plan Amendment Application Form**
Location	Development Services Offices and Legislative Services Offices
Information	Name, signature, property address, telephone number, legal description, permit number, description of development, email address, name and address of sub-contractors used
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Municipal Government Act*

Title	**Municipal Development Plan Amendment Application Form**
Location	Development Services Offices and Legislative Services Offices
Information	Name, signature, property address, telephone number, legal description, permit number, description of development, email address, name and address of sub-contractors used
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Municipal Government Act*

Title	**Subdivision Application Form**
Location	Development Services Offices
Information	Name, signature, property address, telephone number, legal description, permit number, description of development, existing use of land, description of buildings on the land, topography, soil type, email address, name and address of sub-contractors used
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Municipal Government Act*

Title	**Subdivision Application Checklist Form**
Location	Development Services Offices
Information	Name, signature, name, and address of sub-contractors used
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Municipal Government Act*

Title	**Abandoned Well Declaration**
Location	Development Services Offices
Information	Name, signature, property address, name and address of sub-contractors used
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Urban Beekeeping Application**
Location	Development Services Offices
Information	Name, signature, property address, telephone number, legal description, email address, fax number, provincial license or permit number if applicable
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Computer Programs & Software

Title	**eSite (computer software)**
Location	Development Services Offices, Contractor Park Enterprises Ltd, and IT Department Offices/Servers
Information	Name, mailing address, signature, property address, telephone number, fax number, legal description, permit number, name and address of sub-contractors used, construction value, email address, type of work, date of permit inspections, inspection history, details about permit inspections
Individuals	Property owners, applicants, contractors

Use	Administration of Development Services and Building Inspection Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Safety Codes Act*

Title	**ArcReader Maps GIS (computer software)**
Location	Development Services Offices and IT Department Offices/Servers
Information	Name, registered owner, mailing address, property address, telephone number, legal description, assessed value, email address
Individuals	Property owners, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**Great Plains and Microsoft Diamond Software (computer software)**
Location	Development Services Offices and IT Department Offices/Servers
Information	Name, mailing address, signature, property address, telephone number, fax number, legal description, email address, current transactions and receipts with the Town of Strathmore, business licenses, pet licenses, utility bills and transactions
Individuals	Property owners, current and past residents, applicants, contractors
Use	Administration of Development Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy*

IODS - Infrastructure Services

Title	**Citizen Communications Form**
Location	Infrastructure Services Offices and Communication Offices/Town Website
Information	Name, address, telephone number, email address, nature, and location of concern

Individuals	General public, property owners, residents, businesses, contractors
Use	Required for further information and or follow up; to investigate an incident or area of concern noted by the caller; or for reference
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Safety Codes Act*

Title	**Temporary Road and Parking Closure Application**
Location	Infrastructure Services Offices – M-Files
Information	Name, address, telephone number, email address, event description, closure location
Individuals	General public, homeowners, residents, homeowner associations, businesses, contractors
Use	To administer and track permitting for road and parking closures. To assist with making the public aware of road and parking closures.
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Safety Codes Act*

Title	**Cross Connection Control Testing Report**
Location	Infrastructure Services Offices – M-Files
Information	Name, address, telephone number, email address, business address, business type, equipment type
Individuals	General public, homeowners, residents, homeowner associations, businesses, contractors
Use	To administer and track backflow prevention installation
Legal Authority	Water Utility Bylaw No 19-19, Section 4(c) of the *Protection of Privacy* and the *Safety Codes Act*

Title	**Waste Services Tracking Spreadsheet**
Location	Infrastructure Services Offices – M-Files
Information	Name, address, telephone number, email address, nature of the concern
Individuals	Property owners, residents
Use	To administer and track waste service collection concerns

Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Safety Codes Act*

Title	**Water/Sanitary/Sewer Services (EPCOR) Tracking Spreadsheet**
Location	Infrastructure Services Offices – M-Files
Information	Name, address, telephone number, email address, nature of the concern
Individuals	Property owners, residents
Use	To administer and track water, sanitary, and sewer concerns
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Facility Crossing Agreement**
Location	Infrastructure Services Offices – M-Files
Information	Name, address, legal land description, telephone number, email address, business address, information pertaining to project/program
Individuals	Businesses, contractors
Use	Required for further information and or follow up
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Title	**Request for Quotes and Request for Proposals**
Location	Infrastructure Services Offices – M-Files
Information	Name, address, telephone number, email address, business address, information pertaining to project/program
Individuals	Businesses, contractors
Use	Required for further information and or follow up; to facilitate tender reviews and project proponents
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Safety Codes Act*

Computer Programs & Software:

Title	**Cityworks Maintenance Management and Permitting Software**
Location	Infrastructure Services Offices and IT Department Offices/Servers
Information	Name, address, telephone number, email address, nature, and location of concern
Individuals	Property owners, residents, public inquiries, contractors
Use	Administration of Infrastructure Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**ArcReader Maps GIS**
Location	Infrastructure Services Offices and IT Department Offices/Servers
Information	Name, registered owner, mailing address, property address, telephone number, legal description, assessed value, email address
Individuals	Property owners, residents, public
Use	Administration of Infrastructure Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy*

IODS - Operations Services

Title	**Citizen Communications Form and Report a Problem Form**
Location	Operations Services Offices and Communication Offices/Town Website
Information	Name, address, telephone number, email address, nature, and location of concern
Individuals	General public, homeowners, residents, homeowner associations, businesses, contractors, nature, and location of concern
Use	Required for further information and or follow up; to investigate an incident or area of concern noted by the

	caller; or for reference
Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**Truck Haul Approvals**
Location	Operations Services Offices
Information	Name, telephone number, company name, email address
Individuals	Individuals who need to go off a truck route or haul overweight or over-dimensional loads
Use	To administer and track permitting for overweight or over-dimensional loads and approve travel off truck routes
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Safety Codes Act*

Title	**Fats, Oils and Grease Interceptor Service Record**
Location	Infrastructure Services Offices – M-Files
Information	Facility name, address, inspection date, and repair information
Individuals	Businesses, contractors – internal and external
Use	Required for further information and or follow up
Legal Authority	Section 4(c) of the *Protection of Privacy* and the *Safety Codes Act*

Computers Programs & Software

Title	**Cityworks Maintenance Management and Permitting Software**
Location	Operations Services Offices and IT Department Offices/Servers
Information	Name, address, telephone number, email address, nature, and location of concern
Individuals	Property owners, residents, public inquiries
Use	Administration of Operations Services Department/Program

Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**ArcReader Maps GIS**
Location	Operation Services Offices and IT Department Offices/Servers
Information	Name, registered owner, mailing address, property address, telephone number, legal description, assessed value, email address
Individuals	Property owners, residents, public
Use	Administration of Operations Services Department/Program
Legal Authority	Section 4(c) of the *Protection of Privacy*

SAFS – Communication

Title	**Photo/Video Release Form**
Location	Communication Department
Information	Name, signature, phone number, and Address
Individuals	Individuals who have been photographed or recorded on video
Use	Used by Communications for photo or video that may appear on the website, printed material and other mediums used for promotional and educational purposes with permission
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Citizen Communication Forms/ Facebook Messages**
Location	Communication Department
Information	Name, email, phone number, and Address
Individuals	Individuals who have questions/concern for the Town of Strathmore

Use	To allow for follow-up by the department to which the question pertains
Legal Authority	Section 4(c) of the *Protection of Privacy*
Title	**Surveys**
Location	Communication Department
Information	Name, email
Individuals	Individuals who participate in the surveys
Use	Purposes of conducting surveys for the Town
Legal Authority	Section 4(c) of the *Protection of Privacy*

SAFS – Finance Admin

Title	**Cemetery Files**
Location	Finance Department, Stone Orchard, Vault
Information	Name/full legal name, address, phone number, email, age, sex, date of birth, date of death, time of death, place of death, burial permit, company name, will, power of attorney
Individuals	Cemetery lot owner, deceased person, alternate contact, funeral home businesses, monument suppliers, and credit card info
Use	To maintain contact regarding the lot, maintenance concerns, and further interest if there are no burials interred in lot; to track deceased information for records, data, and statistics; to contact funeral home for questions regarding the family and information which may be required to perform a burial; to maintain communication regarding monuments and installation concerns or future maintenance.
Legal Authority	Cemeteries Bylaw, *Cemeteries Act & Regulation* (Alberta); Section 4(c) of the *Protection of Privacy Act*

SAFS – Finance - Assessment and Taxation

Title	**Assessment Roll**
Location	Assessment Department
Information	Roll number, legal description, municipal address of each property (vacant and improved parcel), type of improvement on the parcel, assessment class, liability code, linear property information, taxable status, and school declaration of the homeowner
Individuals	Property owners
Use	To produce the annual assessment roll for the Town of Strathmore
Legal Authority	Sections 302(1) & 303 of the *Municipal Government Act*; Section 4(c) of the *Protection of Privacy Act*

Title	**Assessment Roll Database**
Location	Assessment Department
Information	Property owner name, mailing address and/or telephone number; assessment roll number; use of land; land title changes including property owner name, address; sale price of the property; lease information on commercial and industrial properties including the owner name and telephone number; lessee name; rates paid for the lease
Individuals	Property owners, lessees
Use	To help determine the typical market value of commercial and industrial properties and to produce the annual assessment roll
Legal Authority	Sections 295, 302(1) & 303 of the *Municipal Government Act*; Section 4(c) of the *Protection of Privacy Act*

Title	**Tax Roll Database**
Location	Taxation Department
Information	Legal description; assessment of property; property owner name, address and/or telephone number; tax roll number; customer ID; notes on customer activity and banking information for the Monthly Tax Payment Plan; land title information; mortgage numbers; school support declaration

Individuals	Property owners
Use	To produce a tax notice for property owners and customers who create a MyStrathmore Account
Legal Authority	Sections 328 & 329 of the *Municipal Government Act*; Section 4(c) of the *Protection of Privacy Act*

Title	**Tax**
Location	Great Plains and Microsoft Software, Tax Clerk Files
Information	Names, Addresses and telephone number, land titles, banking information
Individuals	Property owners for the sole purpose of maintaining tax files
Use	To produce a tax notice for property owners
Legal Authority	*Municipal Government Act,* Section 4(c) of the *Protection of Privacy*

SAFS – Finance

Title	**Accounts Receivable**
Location	Accounts Receivable Department (Great Plains, Accounts Receivable Files, M-Files)
Information	Name, address, telephone number,
Individuals	Individuals who have had a receivable account. All homeowner in in the Town of Strathmore.
Use	Accounts Receivable administration (Utility account numbers, tax roll number, dog license numbers)
Legal Authority	Section 4(c) of the *Protection of Privacy Act , Municipal Government Act*

Title	**Accounts Payable**
Location	Accounts Payable Department (Great Plains, Accounts Payable Files, M-Files)
Information	Name, address, telephone number, Invoice amounts

Individuals	Individual supplier of good and services
Use	Accounts Payable administration
Legal Authority	Section 4(c) of the *Protection of Privacy Act* and the *Municipal Government Act*

Title	**Finance**
Location	Finance Department (Great Plains, Files, M-Files)
Information	Name, address, telephone number, Personal banking Information (Bankruptcy), Grant Applications
Individuals	Individual files for bankruptcy. Grant application process
Use	Information is collected for the sole purpose of maintaining the financial records and grant applications
Legal Authority	Section 4(c) of the *Protection of Privacy Act*, *Municipal Government Act*

Title	**Insurance Claims**
Location	Insurance & Risk Management Department
Information	Name, address, telephone number, email address, specific details about the claim (property or personal injury), photos of the site; witness statements; claim and file numbers; property details or vehicle details (including license plate numbers); medical records
Individuals	Individuals with insurance claims, third parties, witnesses
Use	Administration of the insurance program
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

SAFS – Finance – Utilities

Title	**Utility Database**
Location	Utility Administration Department

Information	Property owner name, address and/or telephone, utility account number, historical utility billing data including consumption, connection/disconnection dates, customer ID, notes on customer activity and banking information for the payment plans
Individuals	Utility customers and customers who create a MyStrathmore Account
Use	To produce monthly utility invoices for the property owner and My Strathmore Accounts
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Utility Account Maintenance**
Location	Utility Administration Department
Information	Name, address, phone number, email address, banking information
Individuals	Utility customers
Use	To set up and cancel utility accounts and update database information
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Pre-authorized Payment Database**
Location	Utility Administration Department
Information	Names, addresses, bank account numbers
Individuals	Utility customers
Use	To set up pre-authorized payment
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Utilities**
Location	Great Plains (Diamond), Utility Administration Department
Information	Name, address, phone number, email address
Individuals	All properties in the Town of Strathmore with water, well, sewer and garbage services

Use	To set up and cancel utility accounts and update database information
Legal Authority	*Municipal Government Act* and Section 4(c) of the *Protection of Privacy*

SAFS – Information Technology

Title	**Security Video**
Location	Information Technology Department
Information	Video of security cameras
Individuals	Individuals in Town Building or on Town property monitored by video surveillance
Use	To monitor security in Town buildings and properties and to act upon any criminal behavior
Legal Authority	Section 4(c) of the *Protection of Privacy*

SAFS - Legislative Services

Title	**Subdivision and Development Appeal Board File**
Location	Legislative Services and Planning Departments - Vault and M-Files
Information	Name, address, telephone number, email address, signature, grounds for appeal, disclosure information, tax roll number, payment information and legal description of the subject property.
Individuals	Appellant, applicant, adjacent property owners and other parties related to the appeal
Use	To process an appeal to the Subdivision and Development Appeal Board
Legal Authority	Land Use Bylaw and Section 4(c) of the *Protection of Privacy*

Title	**Assessment Review Board File**

Location	Legislative Services and Assessment Departments - Vault and M-Files
Information	Roll number, subject property address, legal land description, name, email address, address, signature, reasons for complaint and payment information, registered owner's name and signature, agency contact information, signature of agent or representative, reasons for appeal, disclosure information
Individuals	Complainant, registered owners, agents, representatives, and other parties related to the assessment complaint
Use	To process an appeal against an assessment to the Assessment Review Board
Legal Authority	Section 460 of the *Municipal Government Act* and Section 4(c) of the *Protection of Privacy Act*

Title	**Boards and Committee Membership List**
Location	Legislative Services – Vault and M-Files
Information	Name, Address, phone number, email, and application
Individuals	Board and Committee Members
Use	Recruitment, selection, training, and operations of committee/boards
Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**ATIA Requests**
Location	Legislative Services Department - Vault and M-Files
Information	Name, address, telephone number, fax number, email address, mailing address, description of information requested, banking information
Individuals	Individuals submitting requests under the Freedom of Information and Protection of Privacy Act or their representatives
Use	To respond to and process requests for information
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Special Ballot Request**

Location	Legislative Services Department – Vault
Information	Name, address, mailing address, telephone number and email address
Individuals	Individuals who require a special ballot
Use	For processing special ballot requests
Legal Authority	Section 116 of the *Election Act*; Section 4(c) of the *Protection of Privacy Act*

Title	**Physician Sponsorship Grant Agreement**
Location	Legislative Services Department – M-Files
Information	Name, address, mailing address, telephone number and email address
Individuals	Physicians who apply for the sponsorship grant funding
Use	An incentive to bring doctors to the Town of Strathmore
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Physician Incentive Grant Agreement**
Location	Legislative Services Department – M-Files
Information	Name, address, mailing address, telephone number and email address
Individuals	Physicians who apply for the sponsorship grant funding
Use	An incentive to bring doctors to the Town of Strathmore
Legal Authority	Section 4(c) of the *Protection of Privacy Act*

Title	**Nomination Paper and Candidate's Acceptance**
Location	Legislative Services Department – Vault and M-Files
Information	Name, address for notices and document service, signature, telephone number
Individuals	Nominee, nominator, witness, official agent

Use	For administration of election process
Legal Authority	Section 61 of the *Election Act*; Section 4(c) of the *Protection of Privacy*

Title	**Candidate Information Disclosure Form**
Location	Legislative Services Department – Vault and M-Files
Information	Name, address, telephone number, email, photograph
Individuals	Candidate, agent
Use	For administration of election process
Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**Statement of Scrutineer**
Location	Legislative Services Department – Vault and M-Files
Information	Name, address
Individuals	Scrutineers, Candidates
Use	For administration of election process
Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**Campaign Worker Identification**
Location	Legislative Services Department – Vault and M-Files
Information	Name, address
Individuals	Campaign workers
Use	For administration of election process
Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**Vault Records**
Location	Legislative Services Department – Vault and M-Files
Information	Names, Address, telephone numbers
Individuals	Individuals who we hold a contract with the Town, Landowners
Use	Information is collected for the sole purpose of maintaining legal files
Legal Authority	*Municipal Government Act*

Title	**Litigation**
Location	Legal & Risk Management – Vault and M-Files
Information	Names, Addresses, telephone numbers, specific details about the claim, claim and file numbers, solicitor details
Individuals	Individuals who have legally filed suit with the Town or Town matters requiring legal advice
Use	Information collected for the sole purpose of maintaining the legal files
Legal Authority	*Municipal Government Act*

Title	**Request to speak at a Council meeting Form/ Authorization to speak on someone's behalf form**
Location	Legislative Services Department
Information	Name, Address, telephone number, email
Individuals	Individuals who would like to speak at a Council meeting or authorization to speak on someone's behalf
Use	For administration of a Council Meeting
Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**Mayor Invite Request**
Location	Legislative Services Department
Information	Name, telephone number, email

Individuals	Individuals that request the Mayor's attendance
Use	To fulfill the request
Legal Authority	Section 4(c) of the *Protection of Privacy*

Title	**Volunteer application for Boards or Committees**
Location	Legislative Services Department
Information	Name, address telephone number, email
Individuals	Individuals that submit an application to volunteer with the Town
Use	Obtain Volunteers for the Town of Strathmore's Boards and Committee
Legal Authority	Section 4(c) of the *Protection of Privacy*

SCHEDULE "L"

NON-PERSONAL INFORMATION POLICY

Non-Personal Data Policy

*Effective Date: [**INSERT DATE**]*

1. Purpose

This policy establishes rules for creating, using, and disclosing Non-personal data by Town of Strathmore (the "**Town**") Employees (defined below). It ensures compliance with Alberta's *Protection of Privacy Act* (POPA).

2. Scope

This policy applies to all Town appointees, volunteers, students, contractors, service providers, employees, subcontractors, and any other person who performs a service for the Town, whether under contract or as an agent, or otherwise ("**Employees**"), who handle data in the custody or under the control of the Town.

3. Definitions

Non-personal data means data, including data derived from personal information, that has been generated, modified, anonymized, or aggregated so that it does not identify any individual, and cannot reasonably be used to identify or re-identify any individual.

4. Policy Statement

Employees must not create, use, or disclose Non-personal data unless authorized for a permitted purpose and approved through the Town's privacy process. Non-personal data may only be created for:

- research and analysis;
- planning, administering, delivering, managing, monitoring, or evaluating a program or service; or
- purposes prescribed by regulation under POPA.

Creation record. When creating Non-personal data, Employees must, in writing:

- describe the personal information or derived data used to create the Non-personal data;
- describe the purpose for creating the Non-personal data;
- describe the methods of creating the Non-personal data in a manner that allows it to be replicated for auditing purposes; and
- record the assessment done to ensure that the identity of the individual who is the subject of the Non-personal data cannot be identified or re-identified from the Non-personal data.

Data quality assurance. The assessment referred to above must:

- verify and review the effectiveness of the methods used to create the Non-personal data;
- identify and account for potential bias in the non-personal data;
- identify the security classification level of the Non-personal data;
- identify the level of risk of re-identification and security measures taken to reduce the risk; and
- ensure the accuracy and completeness of the Non-personal data if the Non-personal data will be used to inform decisions about programs or services.

5. Responsibilities

Employees: Follow this policy; do not create, use, or disclose Non-personal data without authorization; escalate uncertain cases to the Privacy Officer before treating data as Non-personal.

Privacy Officer: Approve creation requests, maintain creation records, conduct or oversee re-identification assessments, and assign security classifications.

Department Heads: Ensure staff awareness and compliance within their departments.

6. Review

This policy will be reviewed annually or earlier if changes to POPA or the Town's practices require it.

SCHEDULE "M"

SECURITY CLASSIFICATION SYSTEM

Purpose. In compliance with Alberta's *Protection of Privacy Act* ("**POPA**"), this policy establishes a security classification system for all data, including all personal information and non-personal data, in the custody or under the control of the Town of Strathmore.

Application. This policy applies to all Town all Town appointees, volunteers, students, contractors, service providers, employees, subcontractors, and any other person who performs a service for the Town, whether under contract or as an agent, or otherwise, who handle such data.

Classification Tiers

Tier	Definition	Assignment Criteria	Handling & Access Requirements
Public	Information approved for unrestricted public release.	Published municipal records; Town information approved for public disclosure.	May be shared externally. Maintain version control and source integrity.
Personal Information	Recorded information about an identifiable individual, other than Highly Sensitive Personal Information.	Names and contact details, identifying numbers, employment or service records, opinions about an individual, and other recorded information about an identifiable individual. Data derived from personal information that identifies an individual must be classified at least at this tier. Includes non-personal data only where it has been created under POPA s. 21 and classified as confidential because of Town business, security, or contractual sensitivity.	Need-to-know access for authorized Town purposes. Use and disclose only as authorized by POPA or other law and only to the extent necessary. Store in approved access-controlled systems, use secure transfer and limit copies, exports, downloads, and printouts to the minimum necessary. Maintain accuracy and required retention where the information is used to make a decision that directly affects an individual. Dispose of securely under approved procedures. Apply strict safeguards, including encryption at rest and in transit, audit logging, validation testing, minimum necessary copies, secure destruction, and immediate incident escalation.
Town Confidential Information	Confidential Town business, operational, legal, financial, procurement, policy, or administrative information.	Contracts, Town financial or budget documents, procurement records, internal policies, business plans, legal or operational strategy, and other non-public Town business records.	Need-to-know access. Store in approved Town systems and mark as Town Confidential where practicable. External disclosure requires prior approval from supervisor.

Highly Sensitive Personal Information	Personal information requiring the strictest protections because of its sensitivity, vulnerability context, or risk of significant harm if lost, misused, accessed, or disclosed without authority.	Personal information deemed high sensitivity under MReg s. 1: biometric information about an individual, financial information about an individual, and personal information respecting a minor, senior, or vulnerable individual. Also includes data derived from personal information where the source information or resulting data has comparable sensitivity or risk.	In addition to the Personal Information requirements: Limit access to named users or narrowly defined roles. Apply proactive system monitoring and more frequent access-log review, with documented follow-up for anomalous access. Prohibit bulk export, local storage, portable media use, or external transfer unless specifically approved through a documented privacy/security review.

General Rules

1. Classify information at the time of creation or receipt and label accordingly.
2. Store and handle information in accordance with the highest applicable classification level; where a record contains Town Confidential Information together with personal information or data derived from personal information, apply the Personal Information or Highly Sensitive Personal Information tier, as applicable.
3. Reclassify information promptly if its sensitivity changes.
4. Where classification is unclear, classify conservatively at the higher tier and consult the Privacy Officer before use or disclosure.

Human Oversight, Audit, and Validation Measures

Assign one or more qualified Town employees for each system used to create data derived from personal information or non-personal data to:

1. document the system's purpose, data inputs, intended outputs, and classification level before the system is used;
2. review and approve the purpose, input data, matching logic, transformation method, anonymization method, or model-assisted process before the system is used in production;
3. maintain an audit record for each system used to create data derived from personal information or non-personal data, including the source systems, input data categories, user access, processing dates, method used, output generated, and approving reviewer;
4. review access logs and system activity logs on a periodic schedule proportionate to the classification level of the information or data processed by the system;
5. for systems processing Highly Sensitive Personal Information, conduct more frequent access-log reviews and document follow-up for anomalous access, failed access attempts, unusual exports, or processing outside the approved purpose;

6. validate each system before production use to confirm that the system creates only the intended data derived from personal information or non-personal data and does not produce unauthorized, excessive, inaccurate, incomplete, or unreliable outputs;
7. validate the completeness, accuracy, and currency of personal information inputs, particularly where those inputs may affect an individual directly or support a decision-making process;
8. for systems processing Highly Sensitive Personal Information, validate that encryption, access restrictions, audit logging, monitoring, and export controls are functioning as intended before the system is approved for use;
9. document validation results, identified defects, remediation steps, approval decisions, and retesting outcomes, and retain that documentation for Privacy Officer review and audit purposes.

APPENDIX I

ACCESS TO INFORMATION FORM

The personal information collected on this form will be used to respond to your access to information request. This collection is authorized by section 4 (c) of the *Protection of Privacy Act*. For questions about the collection of personal information, contact the Access to Information Coordinator of the public body that has collected the information you are requesting. See instructions on the following page for completing this form

About you	Last Name	First Name	
	Name of Company or Organization (if applicable)		
	Mailing Address		
	City/Town/Village	Province	Postal Code
	Telephone Number (daytime)	Telephone Number (Evening)	
	Email Address		

About your request	**1. What kind of information do you want to access?**	□ General information (An initial fee of $25 is required – see instructions for explanation of fees.) □ Your own personal information (No initial fee is required for personal information.)
	2. To which public body are you making your request?	(Please fill in the name of the public body that has the records you wish to access. For a complete listing of public bodies, consult the Directory of Public Bodies on the Find an ATI Coordinator website at https://www.alberta.ca/lookup/find-an-ati-coordinator.aspx.
	3. Do you want to:	□ receive a copy of the record? OR □ examine the record?

About the information you want to access	**1. What records do you want to access?**	Please give as much detail as possible. (If you want access to your own personal information, be sure to give all your previous names. For another person's information, you must attach proof that you can legally act for that person.)
	2. What is the time period of the records?	Please give specific dates. (See instructions for details.)

Your Signature	Signature	Date
Where to send your request	Send your completed request form, and initial fee if applicable, to the ATI Coordinator of the public body that has the records you wish to access. For contact information, consult the Directory of Public Bodies on the Find an ATI Coordinator website at https://www.alberta.ca/lookup/find-an-ati-coordinator.aspx.	

FOR OFFICE USE ONLY	
Date Received	Request Number
	Comments

You can access many public body records without making a request under the *Access to Information Act.* To determine whether you need to make a request under the Act or if you need help completing the form, contact the ATI Coordinator of the public body to which you are making the request.

How to make a request
To obtain access to a record, a request must:

- be in writing;
- be submitted to the public body the applicant believes has custody or control of the record;
- provide enough detail to enable the public body to locate and identify the record within a reasonable time with reasonable effort; and
- be accompanied by a fee where a fee is required under this Act.

The public body should respond to the request within 30 business days from receiving the request, unless the time to respond to a request has been extended for additional reasonable purposes.

About you
In this part of the form enter:

- your last name, first name and preferred title, if any;
- the name of the company or organization you are representing, if applicable;
- your complete mailing address and contact information so that the public body can contact you about the request;
- an e-mail address, if any, where correspondence may be sent.

About your request
If you need help to find out what records a public body has, contact the ATI Coordinator for the public body.

1. What kind of information do you want to access?
Check general or personal information.
A request for general information is information other than your own personal information (see below). For example, it would include information about a third party.

- There is an initial fee of $25.00.
- For a request to a government department, make the cheque payable to the Government of Alberta.
- For a request to a public body that is not a government department, please consult with the ATI Coordinator for payment information. Do not include your credit card information in the mail or fax.
- Additional fees may apply, if the total cost of processing your request is more than $150, you are asked to pay a 50% deposit.
- The records are provided when the fee is paid in full.

A request for personal information is recorded information about an identifiable individual. A request for personal information can only be made for your own personal information or for personal information of an individual you are entitled to represent.

- There is no initial fee for accessing your own personal information.
- If the cost of photocopying is more than $10, you will be notified of the fee.

Continuing request
You may indicate in a request that the request, if granted, continues to have effect for a specified period of up to 2 years. Contact the ATI Coordinator of the public body if you are making a continuing request.

- The initial fee is $50.00.
- You must pay any additional costs as the information becomes available.

2. To which public body are you making your request?
Enter the name of the public body that you believe has the records that you are requesting.

3. Do you want to receive a copy of the record or examine the record? Check the appropriate box indicating whether you want to receive a copy of the record or examine the record.

About the information you want to access
1. What records do you want to access?

- Be as specific as possible in describing the records.
- If you need more space, continue your description on a separate sheet of paper and attach it to this request form.

If requesting your own personal information, give:

- your full name;
- any other names that you have previously used; and
- any identifying number that relates to the records, such as your employee number, case number or other identification number.

If requesting another person's information, give:

- the person's full name;
- any other name that person may have used on the records;
- any identifying numbers for the person, if you know them; and
- proof that you have authority to act for that person (e.g. guardianship or trusteeship order, power of attorney).

2. What is the time period of the records?
Enter the specific dates or date ranges of the records you want to access (e.g. if you want records for the period January 1, 2023 to August 31, 2024 or you want records from January 2024 to present etc.)

Your signature Sign and date the form.

Where to send your request
Send your completed form, and initial fee if applicable, to the ATI Coordinator of the public body that has the records you wish to access.

Protection of Privacy Act (POPA) PIA Template

Section 26 of the *Protection of Privacy Act* and Section 7 of the *Protection of Privacy (Ministerial) Regulation*

Disclaimer:

The content of this document is informational in nature and does not constitute legal advice.

Information is shared in accordance with Municipal Government Act and is managed in compliance with the Access to Information Act (ATIA) and the Protection of Privacy Act (POPA). If you have any questions about the Town's collection or release of information, please contact the Town of Strathmore's ATI Coordinator at 403-934-3133 or by email at ATIA@strathmore.ca.

Table of Contents

Introduction 3
Common Questions 4
Read Before Completing your PIA 6
A. General Information About the Public Body or Bodies, Existing PIAs, and the Project * 7
B. Details About the Project * 11
C. Information About Your Privacy Management Program (PMP) * 12
D. Identify Personal Information Involved and your Authority to Collect, Use or Disclose the Information* 13
E. Access, Correction, Accuracy, Retention, Disposition * 17
F. Protection of Information * 20
G. Service Providers * 27
H. Project Risk Assessment and Mitigation * 30
H1. General Risks (to be completed for all PIA submissions) * 31
H2. Risks Associated with Cloud Computing 33
H3. Risks Associated with Research 35
Appendix A. **Data Matching** 37
Appendix B. **Common or Integrated Program or Service** 41
Appendix C. **Use of Automated Systems or Other Forms of Innovative Technology** 45
Appendix D. **PIA Cover Letter *** 48
Appendix E. **PIA Submission Checklist *** 50

Introduction

Section 26 of the *Protection of Privacy Act* (POPA) requires the Town of Strathmore (the Town) to prepare a privacy impact assessment (PIA) in prescribed circumstances and, if required by the regulations, submit it to the Commissioner in accordance with the regulations. In addition, as part of the Commissioner's responsibility to monitor how POPA is administered to ensure that its purposes are achieved, the Commissioner may, as described in section 27(1)(j) of POPA, request a copy of a public body's PIA.

Section 7(1) of the *Protection of Privacy Act (Ministerial) Regulation* (M-Regulation) requires the Town of Strathmore to prepare a PIA with respect to a new, or a substantial change to an existing, administrative practice, program, project or service that involves the collection, use or disclosure of personal information if one or more of the following factors requiring the submission of a PIA to the Commissioner apply:

(a) A practice, program, project or service will collect, use or disclose personal information deemed to be of high sensitivity. Section 1 of the M-Regulation deems biometric information about an individual, financial information about an individual, personal information respecting a minor, senior or vulnerable individual to be of high sensitivity.

(b) A practice, program, project or service will involve the personal information of a significant percentage of the population the Town of Strathmore serves.

(c) A practice, program, project or service will involve data matching between two or more public bodies. Section 1(f) of POPA defines "data matching" as linking personal information between two or more databases or other electronic sources of information.

(d) A practice, program, project or service is part of a common or integrated program or service. Section 1(d) of POPA defines "common or integrated program or service" in relation to the Town of Strathmore to mean a program or service planned, administered, managed, monitored or evaluated by (i) the Town of Strathmore working collaboratively with one or more other public bodies, or (ii) another public body working on behalf of (A) the Town of Strathmore, or (B) the Town of Strathmore and one or more other public bodies.

(e) A practice, program, project or service involves the development or use of innovative technology.

The Town of Strathmore is to use this template document when submitting their POPA PIAs to the Office of the Information and Privacy Commissioner (OIPC).

Common Questions

1. What is a PIA?

Generally, a PIA maps the flow of information in a proposed system or practice or project and identifies the legal authority permitting it. A PIA also identifies privacy and security risks and associated mitigating controls.

2. Why is a PIA important, or in some cases, required?

Conducting a PIA prior to implementing a new, or a substantial change to an existing, information system, administrative practice, program, project or service, which will involve the collection, use or disclosure of personal information, assists the Town in identifying and addressing potential privacy and security risks that may occur when processing personal information as part of an electronic information system, administrative practice, data matching or in other circumstances where risks to privacy may result from the processing. It also allows the Town to look at and evaluate information flows to determine if the collection, use and disclosure of the personal information complies with POPA.

3. What if I am not sure if I am required to submit a PIA to the Commissioner?

If the Town is unsure whether it is required to complete a PIA or to complete and submit a PIA to the Information and Privacy Commissioner, the Town should use the PIA Submission Assessment Tool for assistance.

4. Is a public body required to complete PIAs without submitting them to the Commissioner?

Yes, the Town is required to complete PIAs under section 7(1)(a) of the M-Regulation. However, the Town is not required to submit PIAs conducted under 7(1)(a) of the M-Regulation to the Commissioner, but the Commissioner can request copies of those PIAs under section 27(1)(j) of POPA.

5. Can a public body use this PIA template to complete its own PIA pursuant to section 7(1)(a) of the M-Regulation?

Yes, the OIPC recommends that Town use this template for all POPA-related PIAs. For PIAs that must be submitted to the Commissioner under POPA, it is mandatory to use this template. Since the Commissioner can request these PIAs, it is important that the PIAs are completed to meet the PIA requirements under POPA, which is the foundation of this template.

6. What if I am unsure how to answer a question in the PIA template?

This template has a completion guide. The guide assists the Town in completing this PIA template by providing explanations or clarifications, where necessary, for each question asked in the template and by describing what is expected of the Town in each question. We recommend that you complete the PIA template while consulting the **POPA PIA Template Completion Guide.**

If you cannot find answers to your questions in the guide, you may contact the OIPC at **780-422-6860 or 1-888-878-4044 (toll free) or by email at generalinfo@oipc.ab.ca**.

7. This template looks so complicated! Do I have to fill it out completely or to this level of detail?

Section 7(3) of the M-Regulation says a privacy impact assessment must provide a level of detail commensurate with the complexity of the practice, program, project or service that the privacy impact assessment relates to. Using this template when preparing a PIA will assist a public body in meeting this requirement. Don't be intimidated! If you have questions, you can refer to the guide or call our office for assistance. The template has been designed such that it is easy to complete.

Not all sections of this template may apply for a specific project. Consider identifying the sections that apply to the project before completing the PIA.

8. Who is authorized to sign off on POPA PIAs?

Given that section 26(1) of POPA requires the Town to prepare a PIA in prescribed circumstances and, if required by the regulations, submit it to the Commissioner in accordance with the regulations, CAO is legally required to sign off on POPA PIAs. However, section 55(1) of POPA authorizes the CAO to delegate to any person any power, duty or function of the head under the Act, except the power to delegate under this section. Section 55(2) requires that a delegation under subsection (1) be in writing and may contain any conditions or restrictions the CAO considers appropriate. To this end, the Designate of a public body may sign off on the Town's PIA if that Designate has been delegated such a power. A copy of the delegation instrument should be included with the PIA.

Read Before Completing your PIA

IMPORTANT: PIAs that do not have sufficient information will **not** be reviewed by the OIPC. **All sections of this PIA template, whether they apply to your project or not, must be included in your submission. It is important for the OIPC to know that the public body has considered all sections of the PIA template, even though only certain sections may apply to the project under consideration. Do not modify the structure of or reformat the template, including removing any part of the template.**

Note: Consult the POPA PIA Template Completion Guide while completing the PIA.

The term "**project**" when used in this document means any information system, administrative practice, program or service, or a change to any existing information system, administrative practice, program or service the Town plans to implement that will involve the collection, use or disclosure of personal information and which includes one or more of the factors listed in section 7(5)(a) to (e) of the M-Regulation.

What the Town needs to know and have before submitting a POPA PIA to the OIPC

1. **IMPORTANT: Sections A to H of this PIA template are mandatory sections to be completed for all projects. Otherwise, the PIA will be considered incomplete and not accepted for review.**
2. **These sections are marked with an asterisk (*). The template and the PIA Completion Guide will assist you in determining how to answer the questions for your specific project.**
3. **These are mandatory requirements under POPA (referred to as "MUST" in the law) and OIPC project-specific compliance requirements.**
4. The PIA must include a cover letter signed by the *Head of the public body* (Appendix D).
5. Complete Appendix A if the project involves Data Matching. Otherwise indicate that this section does not apply to your project.
6. Complete Appendix B if the project is a Common or Integrated Program or Service. Otherwise indicate that this section does not apply to your project.
7. Complete Appendix C if the project includes the use of an automated system or other forms of innovative technology. Otherwise indicate that this section does not apply to your project.
8. Complete Appendix E – PIA Submission Checklist for all PIA submissions.

Please submit your PIA and the required supporting documentation to the OIPC via PIA@OIPC.AB.CA

For questions that include check boxes, click on the box (☐) to check or uncheck the box.

A. General Information About the Town or Public Bodies, Existing PIAs, and the Project *

1. Does the Town intend to collect, use or disclose personal information as part of this project?

Personal information means recorded information about an identifiable individual. Some examples of personal information include an individual's name, home or business address, home or business email address, race, gender identity, fingerprints and financial history. For a complete listing of what is considered personal information, please see ***section 1(q) of POPA.***

☐Yes ☐No

If yes, proceed to question 2.
If no, there is no requirement under POPA to submit a PIA to the Commissioner for this project.

2. Does the project involve any of the following? (*The first five options are the only prescribed circumstances for which the Town is required to submit PIAs to the Commissioner under section 7(5) of the M-Regulation)*

Select all that apply

☐ A practice, program, project or service will collect, use or disclose personal information deemed to be of high sensitivity *(section 1 of the M-Regulation deems biometric information about an individual, financial information about an individual, personal information respecting a minor, senior or vulnerable individual as personal information that is deemed to be of high sensitivity. See the PIA Completion Guide for more information).*

☐A practice, program, project or service will involve the personal information of a significant percentage of the population the Town serves.

☐A practice, program, project or service will involve data matching between two or more public bodies *(section 1(f) of POPA defines "data matching" as linking personal information between two or more databases or other electronic sources of information.)*

☐A practice, program, project or service is part of a common or integrated program or service *(section 1(d) of POPA defines "common or integrated program or service" in relation to the Town to mean a program or service planned, administered, managed, monitored or evaluated by (i) the Town working collaboratively with one or more other public bodies, or (ii) another public body working on behalf of (A) the Town, or (B) the Town and one or more other public bodies.)*

☐A practice, program, project or service involves the development or use of innovative technology.

☐None of the above (**If you select this option**, you are not required to submit a PIA to the Commissioner)

☐ The loss of, unauthorized access to or unauthorized disclosure of the personal information could result in significant harm.

3. Name and contact information of the public body
   Provide the names and contact information for the public body participating in this PIA.

Name of public body	Name and title of head of public body	Mailing Address of public body	Email Address of head of public body	Telephone number of head of public body

4. Is this a joint PIA with any other public body?

   ☐Yes ☐No

   If yes, complete the table below for each additional participating public body:

Public body	Name and title of head of public body	Mailing Address	Email Address	Telephone Number	Role of Public Body in this PIA

5. Contact information of the person(s) who can answer questions regarding this PIA.
   This individual is responsible for communication with the OIPC during the PIA processing and review process.

   Please complete the table below

Name of contact person	Role of contact person	Mailing address	Email address	Phone number

6. Name or title of the project
   Every project should have a name or title for ease of reference.

7. Is this PIA related to an existing PIA that has been reviewed by the OIPC?

   ☐Yes ☐No

   If yes, please provide the OIPC file number(s) for any related PIAs (if the file is still being processed by the OIPC, please provide the date of submission of the PIA):

8. Is this PIA an amendment to a previously submitted PIA to the OIPC?

   ☐Yes ☐No

   If yes, please provide the OIPC file number(s) for the existing PIA(s) (if the file is still being processed by the OIPC, please provide the date of submission of the PIA):

9. Town of Strathmore file number for this PIA (if applicable)

10. Project implementation date for the project considered for this PIA (**MM/DD/YYYY**)

11. Does this project include any of the following?
Please select all that apply.

☐Data matching –Appendix A of this PIA template must be completed.

☐Common or integrated program or service –Appendix B of this PIA template must be completed. (*A "common or integrated program or service" as described in* ***section 1(d) of POPA*** *means a program or service planned, administered, delivered, managed, monitored or evaluated by the Town working collaboratively with one or more other public bodies,* ***or*** *another public body working on behalf of the public body and one or more other public bodies.)*

☐Automated system (e.g. Artificial Intelligence) that will generate content or make decisions, recommendations or predictions; or another form of innovative technology – Appendix C of this PIA template must be completed, including an Algorithm Impact Assessment (AIA). In addition, ensure that all relevant sections of the PIA template include information regarding the automated system and personal information that will be collected, used or disclosed by the automated system or other innovative technology.
See the POPA PIA Template Completion Guide for additional information about the purpose and details of what is required in an AIA.

☐Cloud computing - Please ensure that all relevant sections of the PIA template include information regarding any cloud computing infrastructure and service providers. In addition, both the H1 and H2 risk tables in section H of the template must be completed.

B. Details About the Project *

12. Provide a detailed description and the purpose of the project including how the collection, use and disclosure of personal information are necessary or related to this purpose or the objectives. ***(The project description should include sufficient detail including technical information about the project. Consider attaching a separate document as necessary.)***

13. Does the project involve the implementation of an electronic information system (EIS)?
An Information System is defined by the National Institute of Standards and Technology (NIST) as a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information." The primary components of electronic information systems typically include hardware, software, database(s) and network(s).

☐Yes ☐No

If yes, identify the name of the system.

14. Are other stakeholders involved in the project that may collect, use or disclose personal information?

☐Yes ☐No

If yes, identify the stakeholders and describe the role of each stakeholder involved in the project, in the space provided below.
List stakeholders that may collect, use or disclose personal information associated with the project or have an impact on the privacy or security of personal information. (e.g. internal business area stakeholders; external stakeholders such as other public bodies participating in a common or integrated program or service, as well as vendors and service providers).

C. Information About Your Privacy Management Program (PMP) *

In this section, we introduce the PMP, as it may assist the Town in completing the PIA by referencing policies and procedures that may be part of the PMP. Since the PMP addresses privacy governance within the Town, the PMP contains valuable information about how the Town upholds the access and privacy rights of individuals whose personal information is collected, used or disclosed in this project.

Section 25 (1) of POPA requires the Tow n to establish and implement a PMP and make it public or provide a copy of the PMP upon request pursuant to section 25 (5). These requirements will come into effect one year after POPA came into force, w hich is on June 11, 2026.

15. Has the Town established and implemented a Privacy Management Program (PMP)?
Section 6 of the M-Regulation describes what the Town must include in its PMP.

☐Yes ☐No

If yes, **enclose a copy of the most current PMP and label it** "**Attachment - Privacy Management Program**". If you have previously submitted a PMP to the OIPC and there has been no change to it since that submission, please provide the OIPC file number for your PMP.

If no, when will the Town finalize and implement its PMP?
The OIPC is working on issuing a POPA PMP Guideline, which will be available on the OIPC website, https://oipc.ab.ca/atia-popa-resources. *As of June 11, 2026, section 25 will come into effect.*

D. Identify Personal Information Involved and your Authority to Collect, Use or Disclose the Information*

16. List the personal information that is collected, used, or disclosed in this project and describe how the Town uses and/or discloses the information **only to the extent necessary to enable the Town** to carry out the identified purposes in a reasonable manner.
Section 12(4) of POPA requires the Town to use personal information only to the extent necessary to enable the Town to carry out its purpose in a reasonable manner. Similarly, section 13(4) of POPA requires the Town to disclose personal information only to the extent necessary to enable the Town to carry out identified purposes in a reasonable manner. If you require additional space to list the personal information, please attach an appendix with the information.

Personal information (e.g. name, date of birth, mailing address, email, etc.)

17. Is personal information collected directly from an individual for this project?

☐Yes ☐No

If yes, provide details regarding how notice is provided to an individual at the time the personal information is collected as part of this project, pursuant to **section 5(2) of POPA**. **Also, provide a copy of the collection notice [enclose with the PIA submission and label it "Attachment 1"].**

18. Does the project use or disclose any personal information with the consent of the individual pursuant to section 12(1)(b) or section 13(1)(c) of POPA, and the requirements of section 2 of the Protection of Privacy Regulation (the Regulation)?

☐Yes ☐No

If yes:

- **Provide a copy of the policy and procedure(s) that address consent [enclose with the PIA submission and label it "Attachment 2"]. OR if you have provided this information to our office as part of your PMP, identify the policy and procedure(s) that address consent in your PMP submission.**

- **Provide a copy of the consent form for use and disclosure of personal information involved in the project [enclose with the PIA submission and label it "Attachment 3"].**

19. Will any personal information about an individual be collected indirectly?

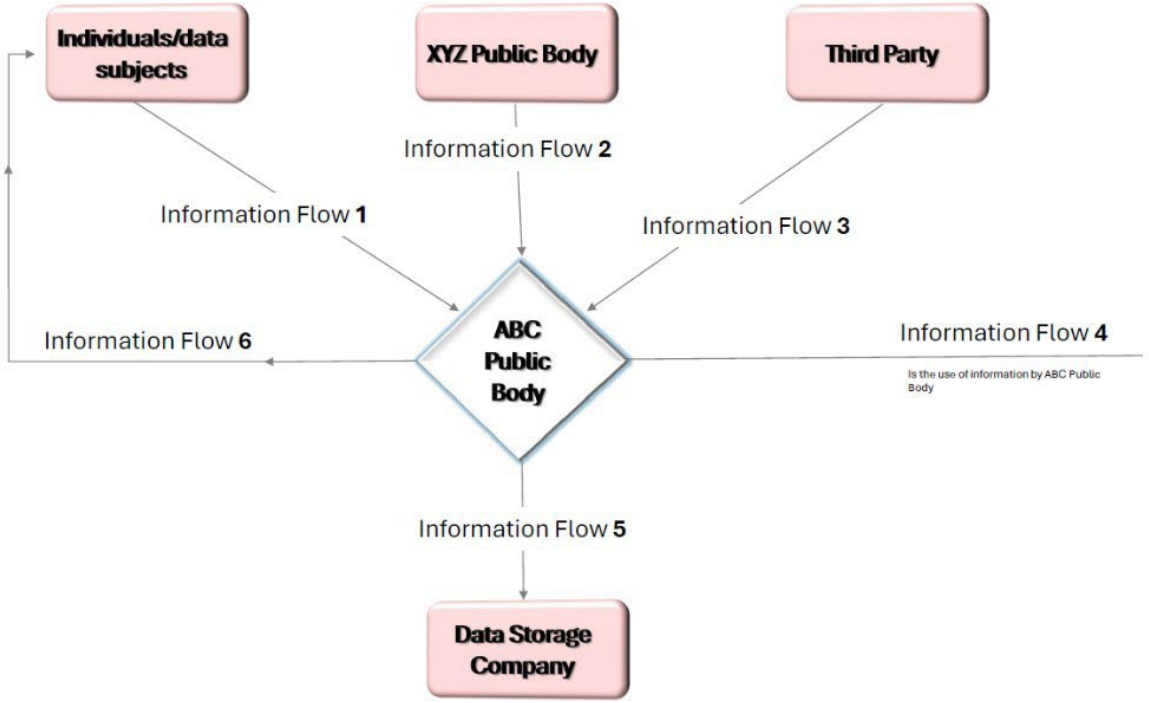
☐Yes ☐No

If yes, explain **how** personal information will be collected indirectly. Ensure you identify the data flow in the information flow diagram and legal authority table below.

20. Information flow diagram

*An information flow diagram illustrates how personal information is collected, used or disclosed in this project. It identifies the various stakeholders and systems associated with the collection, use or disclosure of personal information. The diagram should clearly label each flow with a number, the direction that information is flowing as well as to whom the information is flowing. Note that a project, depending on its complexity, may have more than one information flow diagram. **Note that a business process flow or network diagram is not an information flow diagram. For additional information regarding the differences betw een a netw ork, process flow and data flow diagram, please see the POPA PIA Template Completion Guide.***

See the following information flow diagram example.



Attach a copy of the information flow diagram(s) for this project [enclose with the PIA submission and label it "Attachment 4"].
Note: If an information flow diagram is not attached, the PIA will be deemed incomplete and will not be reviewed.

21. Using the table below, identify and describe the legal authorities and purposes for the collection, method of collection (direct or indirect), use or disclosure of personal information in this project.

The Town is prohibited from collecting (directly or indirectly), using or disclosing personal information except as permitted by sections 4, 12, and 13 of POPA.

Identify each information flow number in your information flow diagram(s) and include the corresponding description of the information in the table below.

Information Flow #	**Description of Information Flow (if the flow is a collection, indicate whether it is direct or indirect collection)** ***Explain how the information flows between parties, systems, etc.***	**Personal Information Involved**	**Stakeholder Involved in the Collection (direct or indirect), Use and/or Disclosure of personal information**	**Purpose for Collection, Use and/or Disclosure**	**Legal Authority for Collection (direct or indirect), Use or Disclosure (cite specific sections of POPA and any other relevant legislation)**
Example flow 1	ABC public body collects personal information directly from	First name, last name, mailing address, email address	ABC public body and individuals	This information is collected from individuals to enroll them into the program	POPA s. 4(c)

Information Flow #	Description of Information Flow (if the flow is a collection, indicate whether it is direct or indirect collection) *Explain how the information flows between parties, systems, etc.*	Personal Information Involved	Stakeholder Involved in the Collection (direct or indirect), Use and/or Disclosure of personal information	Purpose for Collection, Use and/or Disclosure	Legal Authority for Collection (direct or indirect), Use or Disclosure (cite specific sections of POPA and any other relevant legislation)
	the individuals the information is about.			provided by ABC public body.	
1					
2					
3					

E. Access, Correction, Accuracy, Retention, Disposition *

For the questions that ask you to describe certain processes (e.g. describe how an individual can request access to their personal information), ensure the answer to the question includes a fulsome description of the process, rather than limiting the response to a policy name or reference. In addition, explain how the policy referenced applies to the project.

22. Describe how individuals are made aware of their right to access their personal information that is involved in this project and how they can exercise that right.

Section 6 of the Access to Information Act (ATIA) *provides individuals with a right of access to any record in the custody or under the control of the Town, including a record containing personal information about the individuals. Additionally, the right of access enables individuals to know what the Town holds about them in order to assess accuracy or request correction.*

23. Does the Town have an access request policy?

☐Yes ☐No

If yes, and if the Town has provided this information to our office as part of its latest PMP submission, identify the policy and procedure that address access requests in the Town's PMP submission, below; otherwise, provide a copy of the policy and procedure(s) that address access requests **[enclose with the PIA submission and label it "Attachment 5**"].

If no, describe the steps that you are taking to develop and implement such a policy and provide a timeline by which the policy will be in place.

24. Describe how individuals are made aware of their right to request correction of their personal information that is involved in this project and how they can exercise that right.

Section 7 of POPA *provides an individual with the right to request the head of the Town that has the information in its custody or under its control to correct their personal information, if the individual believes there is an error or omission in the individual's personal information.*

25. Does the Town have a correction request policy?

☐Yes ☐No

If yes, and if the Town has provided this information to our office as part of its current PMP submission, identify the policy and procedure that address correction requests in the Town's PMP submission, below; otherwise, provide a copy of the policy and procedure(s) that address correction requests **[enclose with the PIA submission and label it "Attachment 6"]**

If no, describe the steps that you are taking to develop and implement such a policy and provide a timeline by which the policy will be in place.

26. Describe how the Town will ensure that the personal information involved in this project will be accurate and complete?

Section 6 of POPA *requires the Town to make every reasonable effort to ensure personal information that will be used by the Team to make a decision that directly affects an individual is accurate and complete. Examples of methods that the Town may use to ensure personal information is accurate and complete are as follows:*

- *Training and awareness for employees who perform data entry into systems.*
- *Policies and procedures that govern and describe the activities associated with the integrity of personal information.*
- *Configuration of input controls within information systems that ensure correct inputs are accepted by the systems.*
- *Configuration of access controls within information systems that restrict the activities that users may perform on personal information, based on job requirements.*
- *Capturing and reviewing audit logs of activities in a system to detect and address data integrity issues.*
- *Implementing IT change management practices that align with industry standards for changes to information systems.*

27. Has the Town established and implemented a record retention and disposition policy for personal information involved in this project? ***Section 6 (b) of POPA*** *requires that personal information used to make a decision that directly affects an individual be*

retained for at least one year to enable the individual who is the subject of the information to obtain access to the information, or for a shorter period if agreed to in writing by the individual, the Town, and, as applicable, another body that may be involved in records retention.

☐Yes ☐No

If yes, and if the Town has provided this information to our office as part of its current PMP submission, identify the policy and procedure that address record retention and disposition for this project in the PMP submission, below; otherwise, provide a copy of the policy and procedure(s) that address record retention and disposition **[enclose with the PIA submission and label it "Attachment 7"]**.

If no, describe the steps that you are taking to develop and implement such a policy and provide a timeline by which the policy will be in place.

28. if you answered "**yes"** to question 27 and if the project involves the use of an electronic information system to process personal information, describe the steps that the Town has taken to implement the record retention and disposition policy in the electronic information system *(considerations in your response should include but are not limited to indicating whether someone has been assigned the responsibility for the Town's record retention and disposition practices, associated policy and processes as well as describing measures that are in place to demonstrate that the Town is adhering to the policy.)*

F. Protection of Information *

Section 10(1) of POPA *requires the head of a public body to protect personal information in the custody or under the control of the public body by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or*

*destruction. **Section 1 (1)(c) of the Regulation** defines "reasonable security arrangements" as administrative safeguards, physical safeguards and technical safeguards to protect personal information, data derived from personal information and non-personal data in the custody or under the control of the Town that are appropriate and proportional to the security classification level of the information or data, and in the case of non-personal data, ensure, to the extent possible, that the identity of an individual who is the subject of the non-personal data cannot be re-identified from the data. In addition, the **M-Regulation** sets out additional requirements for the security classification of personal information.*

Information about protecting the personal information involved in the project

29. Has the Town assigned a security classification to the personal information involved in the project?
*Section 2 (1) of the M-Regulation requires the Town to assign a security classification level to all personal information, data derived from personal information and non-personal data in the custody or under the control of the public body, based on an internal classification system established by the public body. Section 2 (2) of the M-Regulation requires the security classification level assigned to personal information to reflect the sensitivity of the personal information. Note: This is a **HARD REQUIREMENT**. PIA submissions that do not include information regarding the public body's information security classification system will not be reviewed.*

☐Yes ☐No

If yes, identify and describe the classification level of the information in relation to the public body's information classification system.

If no, the public body must assign a security classification to the personal information involved in the project prior to submitting this PIA.

30. Using the boxes below, describe how the Town will ensure that the personal information involved in this project is protected against such risks as unauthorized access, collection, use, disclosure or destruction **that are appropriate and proportional to the classification of the personal information**.
*Note: This is a **HARD REQUIREMENT**. PIA submissions that do not include information regarding the public body's safeguards will not be reviewed.*

If the project involves a high volume of personal information or highly sensitive personal information, policies and procedures must be documented and attached to this PIA submission as required by section 6(2) of the M-Regulation **[enclose with the PIA submission and label it "Protection of Personal Information Policies and Procedures"]**.
If the policies have been included as part of a PMP submission included in this PIA, include the policy reference (i.e. policy name and page number). However, note that reference to general policies and procedures alone will not be sufficient. Details about how the policies and procedures contribute to the safeguarding of personal information involved **in this project** must also be provided.

a. Describe the administrative safeguards in place to protect the information involved in the project.
Section 1 (2)(a) of the Regulation *describes an "administrative safeguard" as a policy, procedure or practice to manage a public body's conduct that protects the privacy of personal information, data derived from personal information and non-personal data.*
(Some examples of administrative safeguards include documented policies and procedures, security and privacy awareness training, confidentiality agreements, contracts and agreements.)

b. Describe the physical safeguards in place to protect the information involved in the project.
Section 1 (2)(b) of the Regulation *describes a "physical safeguard" as a method to protect a Town's physical assets, including electronic information systems, from natural and environmental hazards and unauthorized intrusion.*
(Some examples of physical safeguards include locked filing cabinets, alarms on premises, locked server rooms, personal information stored out of reach of the public, temperature monitoring and response system, humidity monitoring and response system, fire detection and suppression systems).

c. Describe the technical safeguards in place to protect the information involved in the project.
Section 1(2)(c) of the Regulation *describes a "technical safeguard" as a method to protect a public body's electronic data and access to it.*

(Some examples of technical safeguards include network security controls, application security controls, systems access controls, etc.)

31. Describe how the Town continuously assesses and monitors the safeguards described in the above question to ensure they are working as expected to protect personal information.

32. As it relates to this project, does the Town have a process to ensure its employees are aware of their duty to notify the head of the public body of any loss of, unauthorized access to, or unauthorized disclosure of personal information (**Section 10(2) of POPA**)?

☐Yes ☐No

If yes, describe how the Town makes its employees aware of their duty to notify the CAO of any loss of, unauthorized access to or unauthorized disclosure of personal information (*considerations should include sections of the Town's policies and processes as well as training that ensure employees are aware of the actions to take*).

If no, describe the steps the Town will take to make its employees aware of their duty to notify the CAO of any loss of, unauthorized access to or unauthorized disclosure of personal information involved in this project, and provide a timeline by which this will be done.

Protection of personal information in information systems

Complete this section if the project involves the implementation of an Electronic Information System (EIS).

33. Does the Town have an access control policy and associated procedure(s) that relate to access to personal information in the EIS?
    Note: If the public body is implementing an EIS that processes a high volume of personal information or highly sensitive personal information, this is a HARD REQUIREMENT. PIA submissions that do not include information regarding the public body's access control policy will not be reviewed.
34. Describe the process for approving access to personal information within the information system.

35. Provide details regarding how access is limited to only those employees who have a defined business requirement to access personal information and how their access is limited to only the amount of information required to perform their job duties.

36. Describe the process for revoking access to the information system in a timely manner when such access is no longer required (e.g. employee changes role or employee leaves the organization).

37. Complete the access table, below:

Position or job title	System user role	Number of staff in this role	Permissions assigned to the role (create, read, write, modify, delete, execute, etc.)	Description of information this user can access and description of the actions the user can take (include examples)
(E.g. School Clerk)	(E.g. Admin Support)	(e.g. 2)	(E.g. read, write, modify)	(E.g. school administrative support staff can only view and modify registration information but has no access to student grades)

Logging and Auditing Access to the EIS

38. Does the Town have a logging and auditing policy and associated procedure(s) for this EIS?

Note: If the Town is implementing an EIS that processes a high volume or highly sensitive personal information, this is a **HARD REQUIREMENT**. *PIA submissions that do not include information regarding the Town's access control policy will not be reviewed.*

** If the project involves a high volume of personal information or highly sensitive personal information, a documented logging and auditing policy must be attached to this PIA submission.* **(section 6(2) of M-Regulation)**

☐Yes ☐No

If yes, and if the Town has provided this information to our office as part of its current PMP submission, identify the policy and procedure that address logging and auditing in the Town's PMP submission, below. Otherwise, provide a copy of the policy and procedure(s) that address logging and auditing **[enclose with the PIA submission and label it "Attachment 9"]**.

If no, and the project involves a high volume of personal information or highly sensitive personal information, the Town must develop and document a logging and auditing policy prior to submitting this PIA.

If no, and the project ***does not*** involve a high volume of personal information or highly sensitive personal information, describe the process (or if you have documentation include it) by which the Town logs and audits activities associated with access to personal information stored in the EIS.

39. Does the system capture and maintain audit logs of access to personal information?

☐Yes ☐No

If yes, use the table below to identify the data elements that are captured in the information system's audit logs.

Audit log data elements	**Description**	**Comments (if applicable)**
(E.g. user ID)	(E.g. uniquely identifies a user of the system)	

If no, describe the steps the Town will take to ensure the system captures and maintains audit logs of access to personal information and provide a timeline by which this will be done.

40. Describe the steps taken by the Town to proactively audit access to personal information in the information system.

41. Provide information regarding the audit criteria, the frequency of audits and who conducts the audits.

The Town may consider several factors in determining the frequency to conduct audits, such as the number of users who have access to information in the system, the volume and sensitivity of personal information. Some examples of audit report criteria include, but are not limited to, users accessing the personal information of individuals with the same last name and same physical address, frequently accessed records, frequently failed login attempts, and inactivity audits.

G. Service Providers *

Section 1(h) of POPA *states that an "employee" in relation to the Town, includes "a person who performs a service for the Town as an appointee, volunteer or student or under a contract or agency relationship with the Town". As the Town is ultimately accountable for the actions of its employees in relation to its compliance with POPA, it is important for the Town to enter into contracts or agreements with any third parties that provide services to the Town to ensure each third party complies with POPA. In this section, you will identify the third parties of the Town, the contracts or agreements that are in place and the responsibilities of the third parties regarding privacy and security of personal information. "Person" is defined in the Interpretation Act, section 28(1)(nn) to include a corporation.*

42. Does the Town use service providers, including vendors and contractors, in this project that will have access to personal information or will collect, use or disclose personal information on its behalf? (*The Town must ensure that personal information collected, used or disclosed by the service provider is captured in the information flow diagram and corresponding legal authority table in section D of this PIA.*)

☐Yes ☐No

If yes, proceed and use the table below to provide additional information about the nature of the relationship.
If no, proceed to Section H of the template.

Name of third party	**Relationship with the Public Body**	**Description of services provided**	**Type of agreement or contract that establishes a service provider relationship with public body** *(Documents referenced below must be provided as part of the PIA submission.)*
(E.g. ABC Web Services)	(E.g. Service Provider)	(e.g. web hosting)	(E.g. service agreement)

43. For this project, does the Town have a contractual agreement with its service provider that addresses its duties under POPA as it relates to the service of the service provider, and the privacy and security of personal information under POPA?
Pursuant to section 1(h) of POPA, employee", in relation to the Town, includes a person who performs a service for the Town as an appointee, volunteer or student or under a contract or agency relationship with the Town. This means that a service provider may considered an employee of the Town and must comply with POPA.
Note: If the public body engages the services of third-party service providers, this is a HARD REQUIREMENT. PIA submissions that do not indicate that there is a contract or agreement in place w ith third-party service providers will not be reviewed.

☐Yes ☐No

If yes, proceed to the next question.

If no, the public body must ensure it has a contractual agreement(s) with its service provider(s) that addresses all its compliance obligations under POPA that will be imposed on the service provider to ensure compliance before submitting the PIA.

44. For this project, will the service provider process access to information requests on behalf of the Town?

☐Yes ☐No

If yes, describe the steps that the Town has taken to ensure the contractual agreement with the service provider addresses access to information request processing.

If no, proceed to the next question.

45. For this project, has the Town clarified in its contractual agreement(s) with the service provider(s), that the Town maintains control of any information that the service provider(s) accesses, collects or uses in relation to the services which the service provider(s) provides to the Town?
Note: If the Town engages the services of third-party service providers, this is a **HARD REQUIREMENT**. *PIA submissions that do not include a copy of associated contracts or agreements will not be reviewed.*

☐Yes ☐No

If yes, provide a copy of the agreement(s) and identify the provisions in the agreement that ensure the Town maintains control of the information. **[enclose with the PIA submission and label it "Attachment 10"]**.

If no, the Town must ensure it has a contractual agreement(s) with its service provider that ensures the Town maintains control of information involved with the project before it submits its PIA.

46. Does the contractual agreement(s) in place with the Town's service provider(s) identify each party's responsibilities related to the privacy and security of personal information?

☐Yes ☐No

If **yes**, identify the sections of the agreement(s) that describe the privacy and security provisions, including any provisions that pertain to the collection, use, disclosure, protection, retention of personal information and termination provisions.

If no, describe the steps the Town will take to meet these requirements and the timeframe by which the Town will meet these requirements.

47. Identify sections of the contractual agreement(s) with the service provider(s) that address(es) ongoing training requirements for the employees of the service provider(s) who have access to personal information involved in this project.

H. Project Risk Assessment and Mitigation *

Complete.the.following.privacy.risk.assessment.and.mitigation.table.for.this.project¡.The.risks.listed.under.the.section.are.common.privacy.risks.that.may.exist.in.projects¡.The.Town.is.responsible.for.identifying.all.other.risks.that.may.exist.in.this.project¡

48. Did the Town conduct a security threat and risk assessment (STRA), including a vulnerability assessment (VA) and penetration test (pentest) for the project?

☐ Yes ☐No ☐N/A

If yes, attach copies of the STRA reports including VA and pentest reports and the steps that the Town has taken to address identified security issues **[enclose with the PIA submission and label it "Attachment 11"]**.

If no or N/A, provide clarification as to why a STRA including VA and pentest was not completed or deemed necessary for the project.

H1. General Risks (to be completed for all PIA submissions) *

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Unauthorized collection of personal information by authorized users (e.g. an employee, contractor, vendor, etc.) contrary to section 4 and 5 of POPA	E.g. personal information is collected by the public body and/or the information system is configured to accept personal information that does not relate directly to and is not necessary for the project.		
2.	Unauthorized use of personal information by authorized users			
3.	Unauthorized disclosure of personal information by authorized users.			
4.	Unauthorized access to personal information by unauthorized users or malicious software (e.g. ransomware)			
5.	Loss of personal information			
6.	Loss of custody or control of personal information			
7.	Unauthorized destruction of personal information			
8.	Loss of integrity including unauthorized modification of personal information.			
9.	Unauthorized retention of personal information.			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
10.	Lack of notice or proper notice at the time of collection of personal information collected for this project.			
11.	Lack of clarity or failure to provide information regarding access to or correction of information.			
12.	Lack of or inadequate privacy breach management policies and procedures.			
13.	Lack of assessment by the public body of third parties' (e.g. service providers) privacy and security controls regarding the management of personal information on behalf of the Town			
14.	Use or disclosure of personal information for secondary purposes by the public body or its service providers without proper authority.			
15.	Logging and auditing controls of personal information are insufficient or absent, contrary to section 3(2) of the M-Regulation.			
16.	Lack of human oversight and validation measures for systems, contrary to section 3(2) of the M-Regulation.			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
17.	Failure to conduct a vulnerability assessment to identify and address exploitable security vulnerabilities associated with the implemented system.			
18.	Insert additional risks identified by the public body			

H2. Risks Associated with Cloud Computing

☐ **N/A (check this if it does not apply)**

Complete this section if Town is using or intends to use a cloud computing provider to store or manage personal information as part of this project.

Risk number	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Inadequate segregation and isolation of the public body's cloud environment containing personal information from the cloud provider's other customers in a multi-tenant environment.	E.g., in multitenant cloud environment compromise of one environment could lead to the compromise of other environments due to inappropriate segregation and isolation. In addition, there could potentially be information leakage between environments leading to unauthorize disclosure of personal information.		
2.	Contracts or agreements are either not in place with the			

Risk number	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
	cloud provider or are insufficient.			
3.	The cloud provider does not have a robust privacy and security governance structure.			
4.	Lack of clarity regarding the cloud provider's responsibility to notify the Town of the breach in a timely manner.			
5.	Vendor or cloud provider lock-out.			
6.	Vendor or cloud provider lock-in.			
7.	Unauthorized access to personal information by foreign governments or states.			
8.	The cloud provider uses personal information for purposes not authorized by POPA.			
9.	The cloud provider discloses personal information for purposes not authorized by POPA.			

Risk number	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
10.	Broken authentication and authorization.			
11.	Use of weak cryptographic algorithms or lack of encryption of data in transit and at rest.			
12.	Insert additional risks identified by the public body.			

H3. Risks Associated with Research

☐ **N/A (check this if it does not apply)**

Complete this section if the public body intends to disclose personal information for research or statistical purposes as part of this project.

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Disclosure of personal information for research or statistical purposes is contrary to section 15(a) of POPA.	E.g. the Town fails to assess whether non-identifying data can be used to accomplish the research purpose prior to disclosing individually identifying personal information [s.15(a)(i) of POPA] or the research purpose has not been approved by Commissioner [15(a)(ii) of POPA].		

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
2.	Disclosure of personal information for research or statistical purposes that is not clearly in the public interest, contrary to section 15(b) of POPA.			
3.	Disclosure of personal information for research or statistical purposes that may be harmful to an individual, contrary to section 15(b) of POPA.			
4.	Disclosure of personal information for research or statistical purposes contrary to section 15(c) of POPA.			
5.	Lack of or insufficient research agreement contrary to section 15(d) of POPA and section 4 of the Protection of Privacy Regulation.			
6.	Insert additional risks identified by the Town			

Appendix A. **Data Matching**

Data matching *means linking personal information between 2 or more databases or other electronic sources of information (section 1(f) of POPA). In this section, you will address the Town's intent to carry out data matching and assess whether the Town meets its obligations under POPA related to data matching.*

1. Is the Town carrying out data matching with another public body?

   ☐Yes ☐No

   If yes, complete the rest of Appendix A.
   If no, the Town does not need to complete the rest of Appendix A.

2. What is the purpose(s) for the data matching?
   Section 17 (1) of POPA *authorizes the Town to carry out data matching to create data derived from personal information only for specific purposes.*

   Select all that apply.
   ☐Research and analysis
   ☐Planning, administering, delivering, managing, monitoring or evaluating a program or services
   ☐ One or more prescribed purposes.

3. How does the Town obtain personal information to be used for data matching?
   Section 17(3) of POPA *prohibits the Town from collecting personal information directly from an individual when the collection is for the purposes of data matching; however, the Town may collect personal information from another public body or use personal information in its custody or under its control for data matching purposes.*

   Select all that apply

   ☐Collecting from another public body (proceed to question 4 if this is selected)
   ☐Using personal information in the Town's custody or control (if this is the only option that is selected, proceed to question 7)

4. If the Town is collecting personal information from another public body for the purpose of carrying out data matching, has the Town established a clear governance structure respecting the responsibilities and accountability of each public body involved in the collection of personal information for the purpose of carrying out data matching?
   Section 7(2)(g) of the M-Regulation *requires the Town to establish a clear governance structure if the Town is collecting personal information from another public body under* ***section 17(3) of POPA*** *for the purposes of data matching.*
   Note: This is a HARD REQUIREMENT. PIA submissions that do not include documentation of the governance structure will not be reviewed.
   Note: The governance structure should, at minimum, contain certain requirements as listed in the POPA PIA Template Completion Guide

   ☐Yes ☐No

   If yes, attach documentation related to the governance structure **[enclose with the PIA submission and label it "Attachment 12"]**.
   If no, the Town must implement a clear governance structure that meets the requirements of the M-Regulation prior to submitting the PIA.
5. If the Town is collecting personal information from another public body under section 17(3) of POPA for the purpose of data matching, has the Town entered into an agreement with the other public body from which the Town intends to collect personal information?
   Note: This is a HARD REQUIREMENT. PIA submissions that do not include a copy of the agreement will not be reviewed.
   Note: The agreement should, at minimum, contain certain requirements as listed in the POPA PIA Template Completion Guide. The Town must meet these requirements before submitting their PIAs to the Commissioner for review .

   ☐Yes ☐No

   If yes, attach a copy of the agreement **[enclose with the PIA submission and label it "Attachment 13"]** and identify the sections of the agreement that address the requirements listed in the **POPA PIA Template Completion Guide**.

If no, the Town must enter into an agreement with the other public body prior to submitting this PIA.

6. For the data matching, is the Town submitting this PIA performing any unique collection, use or disclosure of information that only applies to the Town?
   Section 7 (4)(b) of the M-Regulation *authorizes the Town to prepare a joint PIA to describe the data matching, but requires each participating public body to, in addition to the joint PIA, prepare an addendum to address any unique collection, use or disclosure circumstances that apply to that public body.*
   Note: If the Town is performing any unique collection, use or disclosure that only applies to the Town, this is a HARD REQUIREMENT. PIA submissions that do not include a copy of the PIA addendum will not be reviewed.

   ☐Yes ☐No

   If yes, attach a copy of the addendum **[enclose with the PIA submission and label it "Attachment 14"]**
   The Town must prepare an addendum for data matching that meets the requirements of section 7(4)(b) of the M-Regulation and must include the addendum when submitting a joint PIA.

   If no, proceed to the next question.

7. Describe the security arrangements that are in place to protect personal information associated with data matching.
   Section 17 (2) of POPA *requires the Town to carry out data matching in accordance with the prescribed security arrangements in accordance with* ***section 3(1) of the M-Regulation****.* ***Section 3 (1) of the M-Regulation*** *requires the Town to implement reasonable administrative, physical and technical safeguards to protect personal information against such risks as unauthorized access, collection, use, disclosure or destruction. The security arrangements must be appropriate and proportional with the security classification level of that information or data.*
   If the security arrangements that have been described elsew here also apply to the safeguarding of personal information associated w ith data matching, indicate w here in this PIA template and the public body's policy documents this information is captured.

8. Please complete the following Risk Assessment and Mitigation table for risks related to Data Matching

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Failure to establish a clear governance structure respecting the responsibilities and accountability of the Town conducting the data matching and those of the public body from which personal information is collected for the purpose of data matching, if personal information is collected from another public body for the purpose of data matching.	e.g. section 7(2)(g) of the M-Regulation requires the establishment of a clear governance structure respecting the responsibilities and accountability of two public bodies involved in data matching if one public body is collecting personal information for another public body for the purpose of data matching.		
2.	Collection of personal information directly from individuals for the purpose of data matching contrary to section 17(3) of POPA.			
3.	The data matching process or method is not well defined and properly implemented leading to errors in the resulting data.			
4.	Data quality of the source data used for data matching are not adequately assessed and validated leading to data integrity issues in the resulting data.			
5.	Failure to implement reasonable security controls within the data matching environment thereby exposing personal information to			

	potential loss unauthorized access or unauthorized disclosure.			
6.	Failure to establish and implement a data validation or test process to ensure the resulting data set from the data matching process is the desired and accurate outcome.			
7.	Failure to securely remove personal information from the data matching environment upon completion for the data matching process thereby exposing personal information to potential unauthorized access.			
8.	Insert additional risks identified by the public body.			

Appendix B. **Common or Integrated Program or Service**

A "common or integrated program or service" pursuant to ***section 1(d) of POPA*** *means a program or service planned, administered, delivered, managed, monitored or evaluated by the public body working collaboratively with one or more other public bodies,* ***or*** *another public body working on behalf of the public body and one or more other public bodies.*

1. Is the project a common or integrated program or service?

   □ Yes ☐No

   If yes, complete the rest of Appendix B.
   If no, the Town does not need to complete the rest of Appendix B.

2. Is this a new common or integrated program or service or a change to an existing common or integrated program or service?

☐ A new common or integrated program or service
☐ A change to an existing common or integrated program or service

a. List the other public body or public bodies with which the Town submitting this PIA is collaborating or for which the Town submitting this PIA is working on behalf of for the purposes of the common or integrated program or service.

b. If this is a joint PIA submission, identify the public body coordinating the submission of this PIA on behalf of the other public body or public bodies?

c. If this is a change to an existing common or integrated program or service, provide the **OIPC PIA file number** for the existing PIA or identify the date the existing PIA was submitted to the OIPC if it is still being processed by the OIPC and the file number has not yet been issued for the PIA.

3. Has the Town, engaging in a common or integrated program or service with one or more other public bodies, established a clear governance structure respecting the responsibilities and accountability of each public body involved in the common or integrated program or service?
Section 7(2)(g) of the M-Regulation *requires the Town to have a clear governance structure respecting the responsibilities and accountability of each public body if two or more public bodies are engaging in a common or integrated program or service. A governance structure is a documented set of rules and processes that identify the roles, responsibilities, and accountability of each public body participating in the integrated program or service.*
Note: This is a HARD REQUIREMENT. PIA submissions that do not include documentation of the governance structure will not be reviewed.
Note: The governance structure should, at minimum, contain certain requirements as listed in the POPA PIA Template Completion Guide

☐Yes ☐No

If yes, attach documentation related to the governance structure **[enclose with the PIA submission and label it "Attachment 15"]**.

If no, the Town must implement a clear and documented governance structure that meets the requirements of Section 7(2)(g) of the M-Regulation prior to submitting the PIA. The governance structure must have been implemented if the project has been launched or be implemented prior to launching the project if the project is yet to be launched.

4. Has the Town engaged in a common or integrated program or service with one or more other public bodies, entered into an agreement with the other public body or public bodies that addresses how each public body involved in the common or integrated program or service complies with POPA?
Note: This is a **HARD REQUIREMENT**. *PIA submissions that do not include a copy of the agreement will not be reviewed.*
Note: The agreement should, at minimum, contain certain requirements as listed in the POPA PIA Template Completion Guide Public bodies must meet these requirements before submitting their PIAs to the Commissioner for review.

☐Yes ☐No

If yes, attach a copy of the agreement **[enclose with the PIA submission and label it "Attachment 16"]** and identify the sections of the agreement that address the requirements listed in the **POPA PIA Template Completion Guide**.

If no, the Town must enter into an agreement with the other public body or public bodies prior to submitting this PIA.

5. For the common or integrated program or service, is the Town submitting this PIA performing any unique collection, use or disclosure of information that only applies to the Town?

Section 7 (4)(b) of the M-Regulation *authorizes the Town to prepare a joint PIA to describe a common or integrated program or service, but requires each participating public body to, in addition to the joint PIA, prepare an addendum to address any unique collection, use or disclosure circumstances that apply to that public body.*
Note: If the Town is performing any unique collection, use or disclosure that only applies to the Town, this is a HARD REQUIREMENT. PIA submissions that do not include a copy of the PIA addendum will not be reviewed.

☐Yes ☐No

If yes, attach a copy of the addendum **[enclose with the PIA submission and label it "Attachment 17"]**.

The Town must prepare an addendum for any unique collection, use or disclosure applicable to the Town that meets the requirements of section 7(4)(b) of the M-Regulation. The addendum must be included with the PIA submission.

6. Please complete the following Risk Assessment and Mitigation table for risks related to common or integrated programs or services.

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Lack of clear governance for common or integrated program or service contrary to section 7(2)(g) of the M-Regulation.	E.g. governance structure including policies are not in place or are inadequate leading to inconsistencies in the management of the program that creates exploitable privacy and security vulnerabilities.		
2.	Lack of clarity in accountability for different aspects of the program or service.			
3.	Lack of clarity in responsibility for different aspects of the program or service.			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
4.	Lack of alignment between the public body's Privacy Management Program and the governance structure of the common or integrated program or service.			
5.	Lack of transparency regarding how individuals' access and privacy rights are upheld.			
6.	Insert additional risks identified by the Town.			

Appendix C. **Use of Automated Systems or Other Forms of Innovative Technology**

☐N/A (check if this does not apply)

Complete this section if the Town intends to use an automated system, such as Artificial Intelligence (AI) or other forms of innovative technology that generates content or makes decisions, recommendations.

1. Has the Town completed an Algorithmic Impact Assessment (AIA) for this project?
   See the POPA PIA Template Completion Guide for additional information about the purpose and details of what is required in an AIA.

   ☐Yes ☐No

   If yes, **attach a copy of the AIA for this project [enclose with the PIA submission and label it "Attachment 18"]**.

2. Please complete the following Risk Assessment and Mitigation table for risks related to automated systems (e.g. AI) or other forms of innovative technology.

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
1.	Loss of custody or control of personal information in an automated system that is hosted by a third party.	E.g. failure to maintain custody or control of personal information ingested by an AI system due to lack of controls to securely and automatically delete information from the AI system.		
2.	Lack of or insufficient policies and procedures to govern automated systems or other innovative technology implementation.			
3.	Lack of clarity on processes and tools in place to ensure accuracy in an automated system's decision making.			
4.	Lack of clarify on how the quality and reliability of an automated system model training data to minimize bias and inaccurate automated decisions including hallucination.			
5.	Automated system inputs are not validated and securely protected, making the inputs vulnerable to tempering.			
6.	Lack of understanding of what automated system training model (static or dynamic) is implemented and how the model is monitored			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
	and kept up to date to ensure it works within its defined parameters.			
7.	The automated system model is not well adjusted to the training data (underfitting) leading to broad generalization and inaccurate results (false positives) with new data.			
8.	The automated system model is too adjusted to the training data (overfitting) leading to lack of generalization and possible inaccurate or unsatisfactory results using new data results (false negatives).			
9.	The automated system is not securely configured, making it vulnerable to compromise.			
10.	Lack of processes for individuals to be made aware of and appeal automated decisions made by automated systems.			
11.	Insufficient logging and auditing controls associated with the automated system or the innovative technology.			
12.	Lack of monitoring of the automated system or other innovative			

Risk #	Privacy Risk	Description	Risk Mitigation Measures	Policy Reference and Public Body Comments
	technology system to ensure it is functioning as intended.			
13.	Failure to conduct security vulnerability on the automated system or other innovative technology system to identify and address exploitable security weaknesses.			
14.	Additional risks identified by the Town related to automated systems and/or other forms of innovative technology.			

Appendix D. **PIA Cover Letter ***

PIA COVER LETTER WORDING
(Customize the areas highlighted in yellow and attach the cover letter on public body official letterhead)

Submitted electronically

DATE

Information and Privacy Commissioner
Suite 410, 9925-109 Street NW
Edmonton, AB T5K 2J8

Dear {INSERT NAME OF THE INFORMATION AND PRIVACY COMMISSIONER}:

Re: {INSERT TITLE OF PROJECT} – {INSERT PUBLIC BODY FILE #, IF APPLICABLE}

Please find attached our privacy impact assessment (PIA) for the above-named project. I am making this submission in accordance with section 26(1) of the *Protection of Privacy Act* (POPA).

The PIA is current as of this submission to your office. I understand that as things change in our project, I will update the PIA by highlighting the sections that have changed, assessing the privacy impact of the change and submit an updated version to your office. If there are substantive changes, I will submit a new PIA to your office which will replace any initial submission(s).

Sincerely,

{SIGNATURE OF THE HEAD OF THE PUBLIC BODY}

{INSERT NAME AND TITLE OF HEAD (OR DESIGNATRE) OF PUBLIC BODY AND NAME OF THE PUBLIC BODY}

C:

Appendix E. **PIA Submission Checklist ***

Detailed Requirements of the PIA – Mandatory Section of the PIA	
Indicate whether you have completed the following sections of the PIA template. Any sections identified with an asterisk (*) are mandatory.	
Mandatory Section of the PIA Template	**Is the section completed and included?**
Cover Letter (Appendix D) *	☐Yes
Section A *- General Information **about the public body or bodies, existing PIAs, and the project**	☐Yes
Section B * - Details About the Project	☐Yes
Section C * - Information About Your Privacy Management Program (PMP)	☐Yes
Section D * - Identify Personal Information Involved and Collection, Use or Disclosure Authority	☐Yes
Section E * - Access, Correction, Accuracy, Retention, Disposition	☐Yes
Section F * - Protection of Information	☐Yes
Section G * - Service Providers	☐Yes
Section H * - Project Risk Assessment and Mitigation	☐Yes

Detailed Requirements of the PIA – Project-Dependent Sections of the PIA	
Indicate whether you have completed the following sections of the PIA template.	
Project-Specific Section of the PIA Template	**Has the public body considered and completed the following sections?**
Appendix A – Data Matching	☐Yes - completed and included ☐N/A - not completed but considered.
Appendix B – Common or Integrated Program or Service	☐Yes - completed and included ☐N/A - not completed but considered.

Appendix C – Use of Automated Systems or other Forms of Innovative Technology	☐Yes - completed and included ☐N/A - not completed but considered.

Attachments to be enclosed with the PIA	
Indicate whether you have attached the requested attachments (where required) for the project. Any attachments identified with an asterisk (*) are required to be included with your PIA submission.	
Attachment	**Has the public body completed and enclosed the following attachments?**
Privacy Management Program (PMP)	☐Yes ☐No
Protection of Personal Information Policies and Procedures	☐Yes ☐No ☐Included in enclosed PMP
Attachment 1* – Collection Notice	☐Yes ☐Included in enclosed PMP
Attachment 2*- Consent Practices (Policies and Procedures)	☐Yes ☐Included in enclosed PMP
Attachment 3*- Consent Form	☐Yes ☐Included in enclosed PMP
Attachment 4* - Information Flow Diagram	☐Yes ☐Included in enclosed PMP
Attachment 5 - Request to Access Personal Information Practices (Policies and Procedures)	☐Yes ☐No ☐Included in enclosed PMP

Attachment 6 - Correction of Personal Information Request Practices (Policies and Procedures)	☐Yes ☐No ☐Included in enclosed PMP
Attachment	**Has the public body completed and enclosed the following attachments?**
Attachment 7- Record Retention and Disposition Practices (Policies, Procedures, Retention Schedule)	☐Yes ☐No ☐Included in enclosed PMP
Attachment 8 *- Access to Personal Information in EIS Practices (Policies and Procedures) (required where applicable)	☐Yes ☐N/A ☐Included in enclosed PMP
Attachment 9 * – Audit and Logging of Personal Information in EIS (Policies and Procedures) (required where applicable)	☐Yes ☐N/A ☐Included in enclosed PMP
Attachment 10 * – Contracts and Agreements with Third Parties (required where applicable)	☐Yes ☐N/A
Attachment 11 – Third Party and/or Internal Security Testing Results (e.g. vulnerability assessment reports, penetration testing reports, Security Threat and Risk Assessment (STRA) documentation)	☐Yes ☐No
Attachment 12 * - Governance Structure for Data Matching (required where applicable)	☐Yes ☐N/A
Attachment 13 * – Data Matching Agreement (required where applicable)	☐Yes ☐N/A
Attachment 14 *- Data Matching PIA Addendum for Unique Collection, Use or Disclosure by a public body (required where applicable)	☐Yes ☐N/A
Attachment 15 * - Governance Structure for Common and Integrated Programs or Services (required where applicable)	☐Yes ☐N/A
Attachment 16 * - Common or Integrated Programs or Services Agreement (required where applicable)	☐Yes ☐N/A

Attachment 17 * **–** Common or Integrated Programs or Services PIA Addendum for Unique Collection, Use or Disclosure by a public body (required where applicable)	☐Yes ☐N/A
Attachment 18 – Algorithm Impact Assessment	☐Yes ☐No ☐N/A

APPENDIX III

POPA Privacy Forms Package

POPA Privacy Forms Package

Privacy Incident Report Form | Privacy Complaint Form | Correction of Personal Information Form

Prepared for municipal use under Alberta's Protection of Privacy Act (POPA).

These forms are intended to support the Town's Privacy Management Plan and Administrative Directive.

How to Use This Package

- Use the Privacy Incident Report Form internally when there is an actual or suspected loss, unauthorized access, unauthorized collection, unauthorized use, unauthorized disclosure, or unauthorized destruction of personal information.

- Use the Privacy Complaint Form when an individual alleges that the Town improperly collected, used, disclosed, accessed, protected, retained, or disposed of their personal information.

- Use the Correction of Personal Information Form when an individual asks the Town to correct personal information in records in the Town's custody or under its control.

- Do not include unnecessary personal information in forms or emails. Submit forms and attachments through secure channels approved by the Town.

- Where there is a real risk of significant harm (RROSH), the Privacy Officer must assess notification obligations to affected individuals, the Office of the Information and Privacy Commissioner of Alberta, and the Minister responsible for POPA.

Sources and Alignment Notes

- POPA requires Alberta public bodies to establish and implement a Privacy Management Program consisting of documented policies and procedures that promote compliance with POPA.

- Correction requests should be made in writing to the public body with custody or control of the relevant records and should include sufficient detail, the correction requested, reasons, supporting documents, and proof of identity or authority where applicable.

- Privacy complaints should first be submitted to the public body in writing with sufficient detail before an individual seeks OIPC review.

- Privacy incident reporting should capture the public body contact information, incident dates, description, type of incident, types of personal information involved, number of impacted individuals, containment status, mitigation measures, potential harm, and notification status.

- OIPC review processes require the applicable form and supporting documents to be submitted together, and privacy/correction submissions are subject to the OIPC's stated intake requirements and timelines.

Privacy Incident Report Form

Internal reporting form for actual or suspected privacy incidents under POPA

Complete this form as soon as you become aware of an actual or suspected privacy incident.
It is for internal Town use only and must be submitted securely to the Privacy Officer.
Report the incident promptly, even if some details are still unknown.

1. Initial Reporting Information

Town file / reference number	
Date incident reported	
Time incident reported	
Reported by - name, title, department	
Reporter contact information	
Supervisor / manager notified	☐ Yes ☐ No Name: _____
Privacy Officer notified	☐ Yes ☐ No Date/time: _____
IT / Cybersecurity notified, if applicable	☐ Yes ☐ No ☐ Not applicable
Legal / Risk / Insurance notified, if applicable	☐ Yes ☐ No ☐ Not applicable

2. Incident Type

☐ Loss of personal information	☐ Unauthorized access
☐ Unauthorized collection	☐ Unauthorized use
☐ Unauthorized disclosure	☐ Unauthorized destruction
☐ Misdirected email / mail / fax	☐ Lost or stolen device / file
☐ Employee snooping / unauthorized browsing	☐ Cybersecurity event / phishing / ransomware
☐ Vendor / service provider incident	☐ Improper disposal of records
☐ Public posting / publication error	☐ Other: _____

3. Incident Timeline

Date or date range incident occurred	Start: _____ End: _____ ☐ Unknown
Date incident discovered	

How was the incident discovered?	
Was the incident ongoing at discovery?	☐ Yes ☐ No ☐ Unknown
If ongoing, when was it contained?	

4. Factual Description of Incident

Provide a clear, factual description. Avoid speculation. Do not include unnecessary personal identifiers. Attach emails, screenshots, logs, photos, correspondence, or other supporting records where relevant.

_____

_____

_____

_____

_____

_____

_____

_____

5. Personal Information Involved

☐ Name	☐ Age
☐ Date of birth	☐ Gender / gender identity
☐ Race / ethnic origin	☐ Address
☐ Telephone number	☐ Email address
☐ Identifying number	☐ Financial information
☐ Employment information	☐ Educational information
☐ Medical / health-related information	☐ Information about minor(s)
☐ Criminal history / enforcement information	☐ Biometric information
☐ Photograph / video / audio	☐ Location information
☐ Complaint / investigation information	☐ Other: _____

Estimated number of affected individuals	
Does the incident involve minors, seniors, vulnerable persons, or sensitive circumstances?	☐ Yes ☐ No ☐ Unknown
Is the personal information encrypted, password-protected, redacted, or otherwise secured?	☐ Yes ☐ No ☐ Unknown Details: _____
Was the information recovered or deleted by the unintended recipient?	☐ Yes ☐ No ☐ Unknown Evidence: _____

6. Immediate Containment and Mitigation

☐ Email recalled	☐ Recipient contacted and deletion requested
☐ Access disabled / credentials changed	☐ Device located / remote wipe initiated
☐ File or record secured	☐ System isolated
☐ Vendor contacted	☐ Police report filed
☐ Affected program suspended	☐ Records preserved for investigation
☐ Other containment action: _____	

_____

_____

_____

_____

7. Real Risk of Significant Harm (RROSH) Screening

The Privacy Officer must complete or validate the RROSH assessment. Consider sensitivity, misuse, malicious intent, mitigation, number of individuals, vulnerability of affected individuals, and potential harms such as identity theft, financial loss, reputational harm, humiliation, safety risk, legal harm, or damage to relationships.

Is there evidence or reasonable basis to believe the information has been misused?	☐ Yes ☐ No ☐ Unknown
Was the incident caused by malicious intent, theft, hacking, malware, or deliberate misconduct?	☐ Yes ☐ No ☐ Unknown
Is the information highly sensitive?	☐ Yes ☐ No ☐ Unknown

Have mitigation measures reduced the risk of harm?	☐ Yes ☐ No ☐ Unknown
Potential harms identified	☐ Identity theft/fraud ☐ Financial loss ☐ Safety risk ☐ Reputational harm ☐ Humiliation ☐ Employment impact ☐ Legal harm ☐ Other
Preliminary RROSH assessment	☐ RROSH exists ☐ No RROSH ☐ More information required
Assessment completed by	
Assessment date	

8. Notification Decision and Status

Affected individuals notified?	☐ Yes ☐ No ☐ Pending ☐ Not required Date/intended date: _____
OIPC notified?	☐ Yes ☐ No ☐ Pending ☐ Not required Date/intended date: _____
Minister responsible for POPA notified?	☐ Yes ☐ No ☐ Pending ☐ Not required Date/intended date: _____
Insurer / legal counsel notified?	☐ Yes ☐ No ☐ Pending ☐ Not applicable
Reason for notification decision	

9. Service Provider / Third Party Involvement

Was a vendor, contractor, consultant, or external party involved?	☐ Yes ☐ No ☐ Unknown
Name of organization and contact	
Contract / agreement reference	
Has the vendor provided an incident report?	☐ Yes ☐ No ☐ Requested ☐ Not applicable
Contractual breach notice requirements reviewed?	☐ Yes ☐ No ☐ Not applicable

10. Investigation, Corrective Actions and Closure

Root cause	
Corrective actions required	
Responsible owner(s)	
Target completion date(s)	
Follow-up training required?	☐ Yes ☐ No
Policy/procedure/system change required?	☐ Yes ☐ No
Incident closed?	☐ Yes ☐ No Closure date: _____

Role	Name / Title	Signature	Date
Prepared by			
Privacy Officer review			
Department Director / Manager			
Legal / Risk review, if required			

Privacy Complaint Form

For complaints about the collection, use, disclosure, access, protection, retention, or disposal of personal information

Use this form to submit a privacy complaint to the Town.
Under Alberta's POPA process, individuals are expected to first contact the public body in writing with sufficient details before seeking review by the OIPC.
Attach supporting documents where available. Do not include more personal information than necessary.

1. Complainant Information

Last name	
First name	
Middle name	
Organization, if applicable	
Mailing address	
Daytime phone	
Email	
Preferred contact method	☐ Email ☐ Mail ☐ Phone
Preferred accessible format / accommodation, if any	

2. Authority to Act

☐ I am complaining about my own personal information.	
☐ I am acting for another person and have attached proof of authority.	
☐ I am a parent/guardian/trustee/power of attorney.	
☐ Other authority: _____	
Name of person whose information is involved, if different from complainant	
Relationship to that person	
Proof of authority attached	☐ Yes ☐ No ☐ Not applicable

3. Complaint Category

☐ Improper collection of personal information	☐ Improper use of personal information
☐ Improper disclosure of personal information	☐ Unauthorized access or employee browsing
☐ Failure to safeguard personal information	☐ Privacy incident / breach concern
☐ Inaccurate or incomplete personal information	☐ Failure to respond to a privacy concern
☐ Improper retention or disposal	☐ Concern about vendor or third-party handling
☐ Concern about surveillance, recording, or monitoring	☐ Concern about AI, automated system, or data matching
☐ Other: _____	

4. Public Body / Department Involved

Town department / program / facility involved	
Staff member or contact, if known	
Date(s) of incident or concern	
Location, program, or system involved	
Related file, account, permit, ticket, registration, complaint, or incident number	

5. Details of Complaint

Explain what happened, when it happened, how you became aware, what personal information was involved, and why you believe the Town's handling of the information was improper.
Attach copies of correspondence or supporting records where available.

6. Personal Information Involved

☐ Name	☐ Address
☐ Phone number	☐ Email address
☐ Date of birth / age	☐ Identification number
☐ Financial information	☐ Employment information
☐ Health or medical information	☐ Education information
☐ Information about a minor	☐ Image, video, or audio recording
☐ Complaint or investigation information	☐ Other: _____

7. Desired Resolution

☐ Explanation of what occurred	☐ Correction of process or record
☐ Written apology or acknowledgement	☐ Confirmation information has been deleted or secured
☐ Training or policy review	☐ Breach notification review
☐ Other: _____	

_____

_____

_____

8. Supporting Documents

☐ Emails / letters attached	☐ Screenshots attached
☐ Photographs attached	☐ Copies of records attached
☐ Proof of identity attached	☐ Proof of authority attached
☐ Other supporting documents attached	☐ No supporting documents available

9. Declaration and Signature

By signing, I confirm that the information provided in this complaint is true and complete to the best of my knowledge. I understand the Town may need to contact me for clarification and may collect, use, and disclose the information in this form as necessary to investigate and respond to my complaint.

Signature	
Date	

10. Office Use Only

Date received	
Complaint file number	
Identity / authority verified	☐ Yes ☐ No ☐ Not required
Acknowledgement sent	☐ Yes Date: _____
Assigned investigator / Privacy Officer	
Program area notified	
Response deadline / target date	
Outcome	☐ Resolved ☐ Partially resolved ☐ Not substantiated ☐ Corrective action required ☐ Referred
Written response sent	☐ Yes Date: _____
OIPC review rights communicated, if applicable	☐ Yes ☐ No
Closed date	

Notice About OIPC Review

If a complainant is not satisfied with the Town's response, or if the Town does not respond within the applicable period, the complainant may be able to request review by the Office of the Information and Privacy Commissioner of Alberta using the applicable POPA Privacy/Correction Request Form and supporting documents, subject to OIPC intake requirements and timelines.

Correction of Personal Information Form

Request to correct personal information in records in the custody or under the control of the Town

Use this form to request correction of personal information in Town records. Many minor corrections can be handled informally by contacting the department that holds the record.
Complete this form where a formal correction request is required.
Attach proof of identity and any supporting documents.

1. Applicant Information

Last name	
First name	
Middle name	
Other name(s) used in the records	
Organization, if applicable	
Mailing address	
Daytime phone	
Email	
Preferred contact method	☐ Email ☐ Mail ☐ Phone

2. Whose Personal Information Do You Want Corrected?

☐ My own personal information.	
☐ Another person's personal information. Proof of authority is attached.	
Name of individual whose information is to be corrected, if different	
Relationship / authority to act	
Proof of identity attached	☐ Yes ☐ No
Proof of authority attached, if acting for another person	☐ Yes ☐ No ☐ Not applicable

3. Public Body and Record Details

Public body	Town of Strathmore

Department / program / facility believed to hold the record	
Record type	☐ Application/form ☐ Permit/licence ☐ Tax/utility/account record ☐ Enforcement/bylaw record ☐ Recreation/program record ☐ Employment record ☐ Complaint/investigation record ☐ Other
Record date or date range	
File, account, permit, case, employee, or other identifying number	
Where did you see or receive the incorrect information?	

4. Personal Information to be Corrected

Describe the exact information you believe is incorrect or incomplete. Be specific enough for the Town to locate the record. If the name in the record differs from the name above, include the complete name as it appears in the record.

5. Correction Requested and Reason

State the correction you want made and explain why the current information is incorrect or incomplete. Attach evidence that supports the correction, such as official documents, correspondence, account records, court orders, updated forms, or other reliable records.

6. Supporting Documents

☐ Government-issued identification	☐ Proof of authority to act for another person
☐ Official record supporting correction	☐ Correspondence supporting correction
☐ Court order / guardianship / power of attorney	☐ Account, permit, tax, utility, recreation, or employment record
☐ Other: _____	☐ No supporting documents available

7. Declaration and Signature

By signing, I confirm that the information provided is true and complete to the best of my knowledge. I understand the Town may verify my identity or authority and may contact me for clarification. I understand the Town will provide written notice of whether the correction has been made or, if not, whether a note or statement of disagreement will be added to the record where required.

Signature	
Date	

8. Office Use Only

Date received	
Request number	
Received by	
Identity verified	☐ Yes ☐ No ☐ Pending
Authority to act verified, if applicable	☐ Yes ☐ No ☐ Not applicable
Responsible department / record owner	
Record located	☐ Yes ☐ No
Correction approved	☐ Yes ☐ No ☐ Partially
Correction completed date	
If correction refused, statement of disagreement added?	☐ Yes ☐ No ☐ Not applicable
Other public bodies / third parties notified of correction, if required	☐ Yes ☐ No ☐ Not applicable
Written notice sent to applicant	☐ Yes Date: _____
OIPC review rights communicated, if applicable	☐ Yes ☐ No
Closed date	

Comments	

Notice About OIPC Review

If the applicant is not satisfied with the Town's response to a correction request, the applicant may be able to request review by the Office of the Information and Privacy Commissioner of Alberta using the applicable POPA Privacy/Correction Request Form and supporting documents, subject to OIPC intake requirements and timelines.

Version Control

Version	Draft 1.0
Prepared / updated by	
Date	
Reviewed by Privacy Officer	
Reviewed by Legal Counsel	
Approved for use	

APPENDIX VI
OIPC Privacy Breach Notification Form

FOR PUBLIC BODIES

Protection of Privacy Act (POPA) Privacy Breach Notification Form

This form should be used by public bodies to notify the Information and Privacy Commissioner (the Commissioner) of a privacy breach under s. 10(2)(b) of the *Protection of Privacy Act* (POPA).

In this document, a "privacy breach" or "breach" means an incident involving the loss of, unauthorized access to or unauthorized disclosure of personal information in the custody or under the control of a public body where a reasonable person would consider that there exists a real risk of significant harm (RROSH) to an individual as a result of the loss, unauthorized access or unauthorized disclosure.

Notice to the Commissioner must be in writing and include the information listed in s. 4(4) of the *Protection of Privacy (Ministerial) Regulation ("M-Regulation")*.

Prior to completing this form, public bodies should consider completing the POPA Breach Notification Assessment Tool to first assess if they are required to notify the Commissioner of the breach in question. The tool is located at www.oipc.ab.ca.

Free-text fields in this form have character limits. If you need to provide additional information, you may attach the information to this form to a maximum of 15 pages.

Upon completion, please submit this form to breachnotice@oipc.ab.ca.

This form is not for individuals. If you believe your personal information has been lost or improperly collected, used, disclosed, or accessed by a public body go the main page of our website at www.oipc.ab.ca and find "For the Public: Privacy/Correction Complaint" tile on the main page for more information on how to file a complaint with the public body and a review with the Commissioner.

Section A: Information of Public Body	
Date of Notification	
Name of Public Body	
Head of the Public Body	
Public Body's Mailing Address	
Public Body's File Number (if applicable)	

Contact information for a person who can answer OIPC's questions about the breach.	
Name	
Title/Position	
Mailing address	
Telephone number(s)	
Email	

Third party (e.g. a lawyer) notifying the Commissioner of the breach on behalf of the public body (if applicable)	
Name of entity	
Mailing address	
Name of contact person	
Title of contact person	
Telephone number(s)	
Email	
Relationship to Public Body (e.g. lawyer or service provider)	
Is the public body aware of the breach?	
Has the public body authorized the third party to notify the Commissioner on its behalf? Please attach or explain how you are authorized to report on behalf of the public body. (For example, if you are a service provider, is the authorization found in the agreement with the public body?)	

Section B: Breach Description	
1. Date on which or period during which the breach occurred or is thought to have occurred	
2. Date on which the breach was discovered	
3. The manner in which the breach was discovered and, if applicable, the physical location of the breach	
4. Date on which or period during which the breach ended or is thought to have ended	
5. Total number of affected individuals (or estimate if not yet known)	

6. The breach involved (select all that apply):

☐ Loss of personal information

☐ Unauthorized access to personal information

☐ Unauthorized disclosure of personal information

Some examples of situations where a loss of or unauthorized access to or disclosure of personal information occurred are as follows:

- *A loss may occur where an employee misplaces files, loses a laptop containing personal information, or a binder is stolen that contains personal information.*
- *Unauthorized access may occur where an organization's computer system is hacked into by a hacker and personal information is accessed or when an employee accesses personal information for an unauthorized purpose (also referred to as snooping).*
- *Unauthorized disclosure may occur where personal information is sent to the wrong person in error.*

7. Describe the circumstances of the breach including cause, how it was discovered and by whom.

Do not include individually identifying personal information in your description.

This section is very important to determine whether a "real risk of significant harm" or RROSH will likely result due to the breach. Provide a written explanation of the cause of the breach, adding as much detail as possible to assist in the determination of whether a real risk exists.

Click or tap here to enter text.

Section C: Personal Information Involved

8. List the personal information involved in the breach (e.g. name, age, date of birth, Social Insurance Number, medical information, individual's educational, financial, employment or criminal history, home address, email address, telephone number, fingerprints, birth certificate, passport).

Do not include individually identifying information in your description.

If the personal information involved in the breach is sensitive, this is a factor that must be taken into consideration in the RROSH analysis below. The M-Regulation identifies, for example, what is high-sensitivity information for the purposes of the Regulation and includes biometric, financial, and personal information respecting a minor, senior or vulnerable individual.

Click or tap here to enter text.

Section D: Custody or Under Control

9. Describe why you think the public body had "custody or control" of the personal information that was involved in the breach.

In paragraph 39 of Order F2016-64 custody or control refers to an enforceable right of an entity to possess a record or to obtain or demand it, if the record is not in its immediate possession. "Custody or control" also imparts the notion that a public body has duties and rights in relation to a record, such as the duty to preserve or maintain records, or the right to destroy them. See the appendix for more information.

Information is in the custody and control of a public body if the information is stored on a server or in a file cabinet owned by the public body within the public body's premises. If a public body contracts a storage company or cloud provider to store personal information on behalf of the public body, the public body does not have physical custody of the information but maintains control over the information by virtue of an agreement in place with the storage company or cloud provider.

Click or tap here to enter text.

Section E: Significant Harm

10. Describe the harm (damage, detriment, or injury) that may occur to an affected individual as a result of the privacy breach.

Examples of harm includes embarrassment, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identify theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property or other legal harms or financial losses.

Click or tap here to enter text.

11. Describe why the harm that could occur is "significant."

Assess whether, as a result of the breach of personal information, that a "reasonable person" would consider the harm to an individual that could occur, to be significant in nature. For a harm to be significant, it must be important, meaningful and more than trivial consequences or effects. To determine what a "reasonable person" would consider appropriate in the circumstances, you must look beyond your own views and assess whether a reasonable person from the broader community facing similar circumstances would consider the harm suffered to be significant.

A description of "significant harm" in the M-Regulation section 4 includes, but is not limited to, bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identify theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property or other legal harms or financial losses. This is not an exhaustive list as other harms that qualify as significant may apply to the situation.

Click or tap here to enter text.

Section F: Real Risk

12. Describe the public body's assessment of why there is a "real risk" of the significant harm identified in the previous sections to an individual as a result of the loss, unauthorized access or unauthorized disclosure of personal information.

To assess real risk, the public body needs to assess if there is likelihood that the significant harm that will result is more than mere speculation or conjecture. The public body also needs to identify that there is a cause and effect relationship between the breach and the harm for there to be a "real risk" that the harm will occur. This means that the harm must flow directly from the breach.

See the appendix "Assessment of RROSH" for the criteria set out in section 4(1) of the M-Regulation that you are required to take into consideration.

For example: A hacker hacks into your computer system and exfiltrates the personal information (name, address, driver's licence number and Social Insurance Number) of Albertans. In this scenario, it is likely the malicious nature of the third party's actions and/or the lost information (i.e. lost custody or control of personal information) will cause the harm, that is, identity theft. Therefore, in this circumstance, there is a real risk that the harm of identity theft, which is a significant harm, will occur to an Albertan as a result of the theft of the individual's personal information.

Click or tap here to enter text.

Section G: Risk Mitigation

13. Describe the steps the public body has taken to reduce the risk of harm to the affected individual(s) as a result of the privacy breach.

See some examples of mitigating factors that may reduce the risk of harm in the appendix.

Click or tap here to enter text.

14. Describe the measures the public body has taken to prevent a reoccurrence of a similar loss or similar unauthorized access or disclosure of personal information.

Click or tap here to enter text.

Section H: Notice to Affected Individuals

15. Have affected individuals been notified in writing pursuant to s.10(2)(a) of POPA and in accordance with s. 4(3) of the M-Regulation?

☐ Yes (**Attach a copy of the notice.** ***Do not include individually identifying information.)***

☐ In Progress **(Provide the date by which notification will be completed below.)**

☐ No **(Provide the date by which affected individuals will be notified below.)**

Date: Enter date

16. Identify the manner the public body used or intends to use to provide notice to affected individuals of a privacy breach pursuant to section 53(a),(b),(d) and (e) of POPA.
The only authorized manners for providing notice to an affected individual of a privacy breach where there is a RROSH are those listed in section 53 of POPA and as listed in questions 16 and 17 of this form.

Select all that apply:

☐ by prepaid mail to the last known address of the affected individual(s)

☐ by personal service

☐ by fax

☐ in electronic form other than fax e.g. email

17. Does the public body intend to provide notice by substitutional service pursuant to section 53(c) of POPA?

☐ Yes (Any substitutional service must be authorized by the Commissioner).

☐ No

If yes, please describe the method(s) of the substitutional service and provide reasons for using substitutional service and the method(s) selected.

Click or tap here to enter text.

Section I: Notice to Minister

18. Has the Minister been notified in writing pursuant to s. 10(2)(c) of POPA and s.4(5) of M-Regulation?

☐ Yes

☐ In Progress (***Provide the date by which notification will be completed below***.)

☐ No (***Provide the date by which the Minister will be notified below.***)

Date: Enter date

Section J: Additional Relevant Information Regarding the Privacy Breach

19. Has the breach been reported to the police, other authorities, or other public bodies?

☐ Yes (***Provide the name of the entity and the date it was reported.***)

☐ No

Name of entity: Click or tap here to enter text.

Date reported: Enter date

20. Provide any additional relevant information here.

Click or tap here to enter text.

Submitting Breach Notice to the Commissioner

Public bodies are required to notify the Commissioner about a privacy breach under POPA **without unreasonable delay**.

Please submit the completed POPA Privacy Breach Notification Form (minus the appendix) to breachnotice@oipc.ab.ca.

If you are unable to submit the form by email, you can submit it to:

Office of the Information and Privacy Commissioner of Alberta
410-9925 109 Street NW
Edmonton AB T5K 2J8

For more information about privacy breaches, visit https://www.oipc.ab.ca – "Report a Privacy Breach" tile on the main page.

Appendix

Examples of common privacy breaches

Privacy breaches occur in a number of ways. Human error and malicious actions by threat actors can cause privacy breaches. A cybersecurity incident, such as a ransomware or phishing attack, may lead to privacy breaches if personal information is lost, accessed or disclosed as a result of the incident. Some common privacy breaches that have been reported to the Commissioner include:

- Loss or theft of unencrypted mobile devices (e.g. laptops, USB sticks or hard drives) containing personal information.
- Misdirected communications (via email, fax or mail) containing personal information.
- Snooping of (unauthorized access to) patient or customer records by employees (authorized users).
- Ransomware attacks resulting in exfiltration of personal information from a computer system and/or the encryption of the information within the compromised systems thereby preventing authorized users from accessing the information.
- Insecurely disposing of paper records containing personal information by putting the records in a dumpster.
- Disposing of computer systems or storage media without first securely removing personal information stored in them.
- Stolen paper records containing personal information following a break-in into an office, employee's vehicle, or a storage facility.
- Break-in into a record storage facility where paper records containing personal information may not be stolen but accessed by the unauthorized individuals.
- Inadvertent exposure of personal information over the internet due to system misconfiguration.

Custody or Control

- OIPC Order F2016-64 issued by the OIPC, sets out the criteria for determining whether a public body has custody or control:

[Para 40] Previous orders of this office have considered a non-exhaustive list of factors compiled from previous orders of this office and across Canada when answering the question of whether a public body has custody or control of a record. In Order F2008- 023, following previous orders of this office, the Adjudicator set out and considered the following factors to determine whether a public body had custody or control over records:

- Was the record created by an officer or employee of the public body?
- What use did the creator intend to make of the record?
- Does the public body have possession of the record either because it has been voluntarily provided by the creator or pursuant to a mandatory statutory or employment requirement?

- If the public body does not have possession of the record, is it being held by an officer or employee of the public body for the purposes of his or her duties as an officer or employee?
- Does the public body have a right to possession of the record?
- Does the content of the record relate to the public body's mandate and functions?
- Does the public body have the authority to regulate the record's use?
- To what extent has the record been relied upon by the public body?
- How closely is the record integrated with other records held by the public body?
- Does the public body have the authority to dispose of the record?

[para 41] Not every factor is determinative, or relevant, to the issues of custody or control in a given case. Custody or control may be determined by the presence of only one factor. If it can be said, after consideration of the factors, that a public body has an enforceable right to possess records or obtain or demand them from someone else, and has duties in relation to them, such as preserving them, it follows that the public body would have control or custody over the records.

Assessment of RROSH

The RROSH assessment is a reasonable person test. This means what a reasonable person would consider appropriate in given situation or circumstance i.e. where a reasonable person would consider that there exists a RROSH to an individual as a result of the loss, unauthorized access to or unauthorized disclosure of personal information.

Sections 4(1) and (2) of the M-Regulation sets out criteria for assessing RROSH.

4(1) In assessing under section 10(2) of the Act whether there exists a real risk of significant harm to an individual as a result of the loss of, unauthorized access to or unauthorized disclosure of personal information, a public body must consider each of the following factors, in addition to any other relevant factors:

(a) whether there is a reasonable basis to believe that the personal information has been misused or will be misused;
(b) (b) whether the loss of, unauthorized access to or unauthorized disclosure of the personal information occurred as a result of malicious intent;
(c) (c) the sensitivity of the personal information that was lost or accessed or disclosed without authorization;
(d) (d) mitigating measures taken or other factors that reduce the risk of significant harm.

(2) For the purposes of subsection (1), "significant harm" includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, identity theft, negative effects on insurability, negative effects to an individual's credit record, damage to or loss of property or other legal harms or financial losses.

In assessing whether there exists a RROSH to an affected individual from a breach, public bodies must consider all circumstances surrounding the breach including the following:

- What is the nature of the information involved?
- Is the information sensitive?*
- Who obtained or could have obtained access to the information?
- How many persons was the information exposed to?
- Is there any personal or professional relationship between the affected individual and the unauthorized recipient of the information?
- Were there reasonable security controls in place such as encryption to prevent unauthorized access to the information at the time of the breach?
- Were the security controls in place at the time of the breach known to have flaws or vulnerabilities?
- How long was the information exposed to unauthorized individuals?
- Is there evidence of malicious intent associated with the breach such as theft, hacking or malware attack?
- Could the information be used for criminal purposes such as for identity theft or fraud?
- Was the information recovered if it was lost?
- How many individuals are affected by the breach?
- Are there vulnerable individuals involved, such as youth or seniors? Financial information or personal information respecting vulnerable individuals, seniors or minors is considered to be highly sensitive information.
- Can the information be used for targeted attacks such as phishing attack?

* Sensitive personal information may include but is not limited to biometric information, medical information, banking information, ethnicity, race-based information, Social Insurance Number (SIN), passport information, Driver's license information, child custody information, tax information, etc.

Mitigating Factors

Some mitigating factors that may lead to NO RROSH include:

- A stolen mobile device containing personal information was encrypted with an industry standard cryptographic algorithm and the encryption key had not been stolen with the device.
- A stolen mobile device containing personal information was remotely wiped prior to it being accessed.
- A misdirected communication, email or fax, containing personal information was reported by the individual who received the communication in error. In addition, the individual confirmed that the information has been destroyed and has not been disclosed further.
- Personal information that was lost was recovered or returned and there was no malicious intent involved. For instance, a flash drive containing personal information was lost and later recovered and there is evidence that the personal information contained in the flash drive was not accessed.