PRIVACY MANAGEMENT PROGRAM

Protection of Privacy Act (POPA)

Organization:	Lethbridge County
Access and Privacy Advisor:	[Name, Title]
Version:	1.0
Effective Date:	June 10, 2026
Review Date:	_____
CAO Approval:	June 10, 2026
Classification:	Public

This Privacy Management Program (PMP) has been established by Lethbridge County pursuant to Section 25 of the Protection of Privacy Act (POPA) and Section 6 of the Protection of Privacy (Ministerial) Regulation. It documents the governance framework, roles, safeguards, and operational tools that govern how Lethbridge County protects personal information, data derived from personal information, and non-personal data in its custody or under its control. This PMP is supported by five Corporate Directives (LS01 through LS05) which provide the binding operational requirements.

Table of Contents

1. Introduction and Purpose
2. Legislative Framework
3. Scope and Application
4. Relationship to Corporate Directives
5. Privacy Officer Designation
6. Privacy Governance Structure
7. Security Classification System
8. Personal Information Inventory
9. Internal Policies and Procedures — Summary
10. Administrative, Physical and Technical Safeguards
11. Employee Training Requirements
12. Privacy Impact Assessment Process
13. Proactive Monitoring and Risk Management
14. Consent Management
15. Artificial Intelligence and Automated Systems
16. PMP Review and Update Cycle
17. Public Transparency and Availability

Appendix A — Access and Privacy Advisor Designation Form
Appendix B — Personal Information Inventory Template
Appendix C — Delegation of Authority Matrix
Appendix D — Corporate Directives Cross-Reference

1. Introduction and Purpose

This Privacy Management Program (PMP) has been established by Lethbridge County in compliance with Section 25 of the Protection of Privacy Act (POPA) and the Protection of Privacy (Ministerial) Regulation, Section 6. The PMP documents the policies, procedures, and tools that govern how Lethbridge County protects personal information, data derived from personal information, and non-personal data in its custody or under its control.

This PMP is an evolving document that will be updated as legislative requirements change, new programs are implemented, or risks are identified. All employees and contractors of Lethbridge County are bound by this program and by the five Corporate Directives that form its operational foundation.

Objectives

- Promote accountability by establishing clear roles, responsibilities, and processes for managing privacy risks.
- Foster trust with Albertans, employees, and partners by demonstrating a commitment to privacy.
- Specify safeguards to protect personal information, data derived from personal information, and non-personal data.
- Enable risk management tools to identify, assess, and mitigate privacy risks proactively.
- Support service delivery by integrating privacy into County operations while respecting individuals' rights.
- Ensure compliance with POPA and all associated regulations.

2. Legislative Framework

This PMP is grounded in the following legislation and regulations:

Legislation / Regulation	Relevance to This PMP
Protection of Privacy Act (POPA)	Primary legislation establishing privacy rights and obligations for public bodies in Alberta. Requires Lethbridge County to establish and maintain a PMP (s.25) and to comply with obligations respecting collection, use, disclosure, and protection of personal information.
Protection of Privacy (Ministerial) Regulation	Defines requirements for PMPs (s.6), PIAs (s.7), security classifications, reasonable security arrangements, high-sensitivity information (s.1), and privacy incident notification (s.4).
Protection of Privacy Regulation	Defines reasonable security arrangements (s.1(c)), consent rules (s.2), data governance and oversight requirements (s.3).
Access to Information Act (ATIA)	Governs the right of public access to records held by Lethbridge County. Applicable to access requests and interacts with privacy obligations. Addressed in LS01.
Municipal Government Act (MGA)	Establishes the County's governance structure; defines the role of the CAO as Head for purposes of ATIA and POPA.

Key Definitions

Term	Definition
Personal Information	Recorded information about an identifiable individual, as defined in section 1(r) of POPA.
High-Sensitivity Information	Personal information related to biometric information, financial information, or personal information respecting a minor, senior, or vulnerable individual (M-Reg s.1).
Privacy Incident	Loss of, unauthorized access to, or unauthorized disclosure of personal information where a reasonable person would consider there exists a Real Risk of Significant Harm to an individual (POPA s.10(2)).
Real Risk of Significant Harm	Impact to an individual assessed using the factors in M-Reg s.4(1), including bodily harm, humiliation, financial loss, identity theft, and damage to reputation or relationships.
Data Derived from Personal Information	Data created through data matching that identifies an individual whose personal information was used in the data matching.
Non-Personal Data	Data, including data derived from personal information, that has been anonymized so it does not identify any individual, including Synthetic Data (POPA s.1).
Administrative Safeguards	A policy, procedure or practice to manage the County's conduct that protects personal information (Privacy Reg s.1(c)).
Physical Safeguards	A measure to protect the County's physical assets, including electronic information systems, from natural, environmental hazards, and unauthorized intrusion.
Technical Safeguards	A measure to protect the County's electronic information and control access to it.

3. Scope and Application

This PMP applies to:

- Lethbridge County and all its operational units, branches, and divisions.
- All employees, appointees, volunteers, students, contractors, and agents acting on behalf of Lethbridge County.
- All personal information, data derived from personal information, and non-personal data in the custody or under the control of Lethbridge County, regardless of format (paper, electronic, audio, video, etc.).
- All programs, services, administrative practices, and projects undertaken by Lethbridge County that involve the collection, use, or disclosure of personal information.

Third-party service providers who process personal information on behalf of Lethbridge County are required to comply with POPA and this PMP through contractual obligations. Lethbridge County will ensure contractual agreements include privacy and security requirements consistent with POPA and LS05 (Privacy Governance, Safeguards & Information Security).

4. Relationship to Corporate Directives

This PMP establishes the overarching governance framework for privacy management at Lethbridge County. The operational requirements — the binding rules, procedures, responsibilities, non-compliance consequences, and delegation of authority — are set out in five Corporate Directives that form an integrated suite with this PMP.

The directives commit Lethbridge County to the legislative requirements (the "what"); the Procedures associated with each directive provide the operational detail (the "how"). Together, this PMP and its directives satisfy the requirements of Section 25 of POPA and Section 6 of the Protection of Privacy (Ministerial) Regulation.

LS01 Access Privacy Roles Delegation
Establishes the CAO as Head, the Delegated Head, and the Access and Privacy Advisor (Privacy Officer). Contains the full ATIA and POPA Delegation of Authority tables (Schedules A and B) with specific legislative section references. References: POPA s.55; ATIA s.87.

LS02 Individual Rights Consent
Establishes the framework for responding to access requests, correction requests, and privacy complaints within legislated timelines. Sets out the forms of consent (oral, written, electronic) established by the CAO as Head under Privacy Reg s.2. References: POPA Part 2–4; Privacy Reg s.2.

LS03 Privacy Incident Response & Privacy Impact Assessments
Establishes the mandatory incident response process, including the Real Risk of Significant Harm assessment (M-Reg s.4(1)), notification obligations, and root-cause analysis requirements. Establishes the PIA process, OIPC submission requirements, and PIA Registry. References: POPA s.10, s.26; M-Reg s.4, s.7.

LS04 Data Management & Artificial Intelligence
Governs creation, use, and disclosure of non-personal data and data derived from personal information. Establishes requirements for AI and automated systems: PIA prior to deployment, human oversight, accuracy monitoring, and the AI and Automated Systems Register. References: POPA s.17–24; M-Reg s.5, s.7; Privacy Reg s.3(2).

LS05 Privacy Governance, Safeguards & Information Security
Establishes the security classification system (Levels 1–4), mandatory privacy training requirements, and administrative, physical, and technical safeguards. Formalizes the Privacy Officer role and the Personal Information Inventory. References: POPA s.25; M-Reg s.6(1)(a), s.6(1)(d)–(f); Privacy Reg s.1(c).

Where this PMP and a Corporate Directive address the same subject, the Corporate Directive governs. Procedures documents associated with each directive provide the step-by-step operational guidance.

5. Privacy Officer (Access and Privacy Advisor) Designation

Pursuant to Section 25 of POPA and Section 6(1)(a) of the Ministerial Regulation, the CAO as Head must designate or identify a Privacy Officer responsible for ensuring organizational compliance with POPA. At Lethbridge County, this role is held by the Access and Privacy Advisor, as formally established in LS01.

Access and Privacy Advisor:	Candice Robison, Legislative Coordinator & Executive Assistant
Department:	Legislative Services
Contact Email:	crobison@lethcounty.ca
Contact Phone:	403-380-1585
Designated By:	Chief Administrative Officer
Effective Date:	June 11, 2026

Access and Privacy Advisor Responsibilities

- Develop, implement, and maintain this PMP and the associated Corporate Directives.
- Ensure organizational tasks and responsibilities under POPA are incorporated into operational structures.
- Report to senior leadership on POPA compliance, privacy risks, and mitigation strategies.
- Act as the primary point of contact for the Office of the Information and Privacy Commissioner (OIPC).
- Oversee PIA completion and submission processes in accordance with LS03.
- Manage privacy incident response in accordance with LS03.
- Coordinate mandatory employee privacy training in accordance with LS05.
- Maintain the Personal Information Inventory, PIA Registry, and AI and Automated Systems Register.
- Respond to requests for the PMP and for personal information access and corrections within legislated timelines.

6. Privacy Governance Structure

The following table documents the privacy roles and responsibilities at Lethbridge County. Detailed delegation of authority, including specific ATIA and POPA section references, is set out in the Delegation Tables in LS01 (Schedules A and B).

Role	Privacy Responsibilities
Chief Administrative Officer / Head	Ultimate accountability for POPA compliance. Designates Access and Privacy Advisor. Approves PMP and all Corporate Directives. Retains or delegates authority under POPA s.55 and ATIA s.87.
Delegated Head (County Manager, Legislative Services)	Responsible for day-to-day oversight of ATIA and POPA compliance on behalf of the CAO.
Access and Privacy Advisor (Privacy Officer)	Develops and maintains the PMP and directives. OIPC liaison. PIA oversight. Privacy incident response. Training coordination. Maintains all PMP registries.
Senior Leadership / Management	Champion privacy culture; ensure program resources are available; review privacy risk reports.
Program Managers	Identify privacy risks in programs; notify Access and Privacy Advisor before new programs or substantial changes; support PIA completion; enforce compliance in their areas.
All Employees and Contractors	Follow this PMP and all Corporate Directives; complete mandatory training; immediately report privacy incidents to the Access and Privacy Advisor.
IT / Information Management	Implement technical safeguards; manage information systems; support PIA technical sections; maintain AI and Automated Systems Register entries.
Legislative Services	Provides legal advice on POPA and ATIA obligations; reviews third-party agreements for privacy and security compliance.

7. Security Classification System

Pursuant to Section 6(1)(d) of the Ministerial Regulation and as detailed in LS05, Lethbridge County has established the following security classification system for all personal information, data derived from personal information, and non-personal data. Information must be classified upon creation or receipt.

Level	Description	Examples	Minimum Safeguards (see LS05, s.7.3–7.5)
Level 1 Public	Non-sensitive information available to the public. No harm if disclosed.	Published reports, public directories, approved County bylaws.	Standard access controls.
Level 2 Protected A	Low-sensitivity personal information. Limited harm if disclosed.	Names, work contact info, general correspondence.	Access controls; privacy training for handlers.
Level 3 Protected B	Moderate-sensitivity. Significant harm if disclosed.	Home addresses, health information, employment records.	Encryption in transit and at rest; restricted role-based access; audit logging.
Level 4 Protected C (High Sensitivity)	High-sensitivity per M-Reg s.1. Severe harm if disclosed. Biometric, financial, or information about minors, seniors, or vulnerable individuals.	Biometric data, SIN numbers, financial accounts, child welfare records.	Strict role-based access; encryption; audit trails; PIA required before program begins; OIPC submission required.

Classification decisions are recorded in the Personal Information Inventory (see Section 8). Retention and destruction schedules must align with classification levels. Full safeguard requirements for each level are set out in LS05, Sections 7.3–7.5.

8. Personal Information Inventory

Pursuant to Section 6(1)(c) of the Ministerial Regulation, Lethbridge County maintains a Personal Information Inventory. This inventory is used to:

- Identify and document all personal information holdings across County programs and systems.
- Support compliance with POPA collection, use, and disclosure limitations.
- Inform security classification and safeguard decisions consistent with LS05.
- Support PIA processes and privacy risk assessments required by LS03.
- Facilitate responses to access and correction requests under LS02.

The Personal Information Inventory is maintained by the Access and Privacy Advisor and reviewed annually or when significant program changes occur. See Appendix B for the inventory template.

9. Internal Policies and Procedures — Summary

Section 6(1)(b) of the Ministerial Regulation requires Lethbridge County to maintain written policies and procedures addressing the following areas. Each area is governed by the applicable Corporate Directive, with associated Procedures providing step-by-step operational guidance. A summary is provided below; the Corporate Directives are the binding instruments.

Subject Area	Governing Directive	Key Requirements
Access and Correction of Personal Information	LS02 (s.7.1, 7.2)	Respond to access requests within legislated timelines. Correct inaccurate information or attach notation. Log all requests and outcomes.
Privacy Incidents	LS03 (s.7.1)	Immediate reporting; containment; Real Risk of Significant Harm assessment; OIPC notification where required; root-cause analysis for significant incidents.
Privacy Complaints	LS02 (s.7.3)	Acknowledge within 5 business days. Written decision within 30 business days. Retain all records.
Non-Personal Data	LS04 (s.7.1)	Document de-identification method; prevent re-identification; restrict third-party disclosure; human oversight for data-creating systems.
Automated Systems and AI	LS04 (s.7.2)	PIA before deployment; no final decisions affecting individuals without human oversight; accuracy monitoring; AI Register maintained.
Consent Management	LS02 (s.7.4)	Obtain informed, voluntary, specific consent before collecting PI where required. Oral, written, and electronic forms established by CAO. Records maintained per retention schedule.
Privacy Impact Assessments	LS03 (s.7.2–7.3)	Required before new or substantially changed programs. OIPC submission for specified triggers. PIA Registry maintained.
Security Classification and Safeguards	LS05 (s.7.1–7.5)	All information classified upon creation. Safeguards proportional to level. Administrative, physical, and technical safeguards documented.
Privacy Training	LS05 (s.7.2)	Mandatory foundations training before handling PI, and annually. Role-specific training for APA, program managers, IT, AI users. Completion records maintained.
Delegation of Authority	LS01 (Schedules A and B)	Full ATIA and POPA delegation tables with section references. Delegations in writing; acting roles formally documented.

10. Administrative, Physical and Technical Safeguards

Pursuant to Section 6(1)(e) of the Ministerial Regulation, Lethbridge County has implemented safeguards proportional to the sensitivity and volume of personal information held. Full safeguard requirements are set out in LS05, Sections 7.3–7.5. A summary is provided below.

10.1 Administrative Safeguards

- This PMP and the five Corporate Directives (LS01 through LS05) constitute the core administrative safeguard framework.
- Confidentiality obligations included in all employment contracts, contractor agreements, and volunteer agreements.
- Mandatory privacy training for all employees and contractors (see Section 11 and LS05).
- Regular privacy risk assessments and PIAs (see Section 12 and LS03).
- Third-party vendor agreements requiring POPA compliance consistent with LS05.
- Information retention and destruction schedules aligned with security classification levels.
- Privacy incident response procedures (see Section 12 and LS03).
- Regular PMP and directive review and update cycles (see Section 16).

10.2 Physical Safeguards

- Secure storage of physical records containing personal information (locked cabinets, secured rooms).
- Access controls to areas where personal information is stored or processed.
- Clean desk standard where personal information is handled.
- Secure disposal of physical records (cross-cut shredding or certified destruction services).
- Physical security controls for electronic information systems (server rooms, workstations).
- Environmental controls protecting against fire, flooding, and power failure.

10.3 Technical Safeguards

- Role-based access controls — access limited to employees with a documented business need.
- Multi-factor authentication for systems classified at Level 3 (Protected B) and above.
- Encryption of personal information in transit (TLS/SSL) and at rest for Level 3 systems and above.
- Audit logging of access to and modifications of personal information systems.
- Endpoint protection (antivirus, anti-malware, endpoint detection and response) on all devices.
- Patch management and vulnerability management programs.
- Network security controls (firewalls, intrusion detection/prevention systems).
- Annual vulnerability assessments for systems classified at Level 3 and above.

11. Employee Training Requirements

Pursuant to Section 6(1)(f) of the Ministerial Regulation, all employees (including contractors, volunteers, students, and appointees) of Lethbridge County must undergo privacy training as required by LS05, Section 7.2. A summary is provided below.

Training Type	Content	Audience	Frequency
POPA Foundations	POPA obligations, individual rights, PMP overview, how to identify and report privacy incidents, consequences of non-compliance.	All employees and contractors	Within 30 days of commencement; annually thereafter
Privacy Incident Response	Identify and report incidents; Real Risk of Significant Harm; the five-step response process in LS03.	All employees	Annually
Role-Specific Privacy Training	Detailed obligations relevant to specific job functions (program managers, IT, AI users).	Program-specific staff	Upon role assignment; as updated
PIA Training	When PIAs are required; how to complete PIAs; OIPC submission process per LS03.	Access and Privacy Advisor, Program Managers	Upon assignment; when LS03 updated
AI and Automated Systems	Privacy obligations for AI tools; PIA requirement; human oversight; LS04 requirements.	IT, data analysts, program leads	Before deploying any AI system; annually

Training completion records are maintained by the Access and Privacy Advisor. Non-compliance with training requirements is reported to the relevant supervisor in accordance with LS05, s.7.2.

12. Privacy Impact Assessment Process

The PIA process is established in LS03. This section provides a summary for reference. The directive governs.

When a PIA Is Required (LS03, s.7.2)

A PIA must be completed before implementing any new, or substantially changed, administrative practice, program, project, or service where one or more of the following apply (M-Reg s.7(1)):

- The loss, unauthorized access, or disclosure of personal information could result in significant harm;
- The practice involves High-Sensitivity personal information (biometric, financial, or information about minors, seniors, or vulnerable individuals);
- The practice will involve the personal information of a significant percentage of the population Lethbridge County serves;
- The practice involves data matching between two or more public bodies;
- The practice is part of a common or integrated program or service; or
- The practice involves the development or use of innovative technology.

PIA Process Steps

Step	Action	Responsible
1. Identify	Program manager identifies that a new or changed program may require a PIA and notifies the Access and Privacy Advisor.	Program Manager
2. Confirm	Access and Privacy Advisor confirms whether a PIA is required using the PIA Assessment Tool.	Access and Privacy Advisor
3. Complete	PIA completed using the OIPC POPA PIA template (where OIPC submission is required) or the County's internal PIA tool.	Program Manager + Access and Privacy Advisor
4. Review	Access and Privacy Advisor reviews the completed PIA for sufficiency and legislative compliance.	Access and Privacy Advisor
5. Submit	Where required (high-sensitivity, high-volume, data-matching, common/integrated programs, or innovative technology), PIA submitted to OIPC using OIPC template.	Access and Privacy Advisor
6. File	Approved PIA filed in the PIA Registry. Registry updated with OIPC reference number, submission date, and next review date.	Access and Privacy Advisor
7. Review	PIAs reviewed when substantial changes occur. Amendments replace relevant portions; addendums used for joint PIAs.	Access and Privacy Advisor + Program Manager

If the OIPC requests a copy of a PIA under POPA s.27(1)(j), Lethbridge County must provide it within 30 business days. The Access and Privacy Advisor coordinates this response.

13. Proactive Monitoring and Risk Management

Pursuant to Section 6(2)(c) of the Ministerial Regulation, and as required by LS03 (s.7.3.4):

- The Access and Privacy Advisor conducts regular reviews of information systems holding personal information to assess security measures and identify emerging risks.
- Privacy risk assessments (including PIAs and Security Threat Risk Assessments) are incorporated into Lethbridge County's organizational risk management processes.
- A privacy risk register is maintained by the Access and Privacy Advisor, documenting identified risks, risk owners, mitigation strategies, and timelines.
- Proactive monitoring activities include: access log reviews, vulnerability scans, security assessments, and third-party compliance reviews.
- Monitoring results are reported to senior leadership at least annually.
- All monitoring activities are conducted in accordance with POPA and applicable legislation.

14. Consent Management

The consent management framework is established in LS02 (s.7.4), pursuant to Section 6(2)(d) of the Ministerial Regulation and Section 2 of the Protection of Privacy Regulation. This section summarizes the framework; the directive governs.

Where POPA requires consent for the collection, use, or disclosure of personal information, Lethbridge County obtains informed, voluntary, and specific consent before proceeding. The CAO as Head has established the following forms of consent as acceptable, consistent with Privacy Reg s.2:

Consent Type	Acceptable For	Documentation Required
Written Consent	[Specify: e.g., high-sensitivity personal information, data matching, research.] Required at minimum for all Level 4 (Protected C) information.	Signed consent form retained on file; copy provided to the individual.
Electronic Consent	[Specify: e.g., online County service applications and digital intake forms.] Subject to authentication and audit trail requirements.	System records date, time, and content; individual can view what they consented to.
Oral Consent	[Specify: e.g., telephone-based service delivery.] Must be contemporaneously documented.	Employee records consent in the relevant system or case file immediately, noting date, time, and purpose.

Consent records are retained per the applicable retention schedule. Individuals are informed at time of consent of their right to withdraw and the consequences of doing so.

15. Artificial Intelligence and Automated Systems

The AI and automated systems framework is established in LS04, pursuant to Sections 6(1)(b)(v) and 6(2)(f) of the Ministerial Regulation. This section summarizes the framework; the directive governs.

- A PIA must be completed and approved by the Access and Privacy Advisor before any AI tool or automated system that processes personal information is deployed or substantially changed.
- Employees must notify the Access and Privacy Advisor before procuring or deploying any AI or automated system.
- AI and automated systems must not make final decisions that significantly affect individuals without meaningful human oversight and a documented review process.
- Personal information used in AI systems must be collected, used, and disclosed only as authorized by POPA.
- Data derived from personal information created by AI systems is subject to all POPA obligations and LS04.
- The accuracy and reliability of AI system outputs affecting individuals must be monitored and validated on a regular, documented basis.
- The Access and Privacy Advisor maintains the AI and Automated Systems Register documenting all such systems and their privacy safeguards.

16. PMP Review and Update Cycle

Pursuant to Section 6(1)(g) of the Ministerial Regulation, Lethbridge County has established the following review cycle for this PMP and the Corporate Directives:

Review Trigger	Review Scope	Responsible	Timeline
Annual Review	Full review of all PMP components and directives; update to reflect legislative changes, new programs, and emerging risks.	Access and Privacy Advisor	Annually
Legislative Change	Review and update affected PMP sections and directives.	Access and Privacy Advisor + Legislative Services	Within 90 days of change taking effect
Significant Privacy Incident	Review and update affected procedures and safeguards following incident investigation.	Access and Privacy Advisor	Within 30 days of completing investigation
New Technology / AI System	Review technical safeguards and LS04 requirements prior to system deployment.	Access and Privacy Advisor + IT	Before deployment
Organizational Change	Review governance structure, roles/responsibilities, and delegation tables in LS01.	Access and Privacy Advisor + HR / Legal	Within 60 days of restructuring

17. Public Transparency and Availability

Pursuant to POPA Section 25 and Section 6 of the Ministerial Regulation:

- Any person may request a copy of this PMP from Lethbridge County.
- Requests must be responded to within 30 business days.
- Lethbridge County may withhold technical information that could compromise the security of personal information in its custody or under its control.
- As a best practice, Lethbridge County will proactively disclose this PMP on the County website at: www.lethcounty.ca.
- The PMP must be made available within 1 year of POPA enactment (by June 11, 2026).

The Corporate Directives (LS01 through LS05) are approved by the CAO and are also available to the public upon request. Technical security information within those directives may be withheld.

Access and Privacy Advisor Designation Form

Protection of Privacy Act (POPA), Section 25 | LS01

I, Cole Beck, Chief Administrative Officer of Lethbridge County, hereby designate / identify the following individual as the Access and Privacy Advisor (Privacy Officer) for Lethbridge County, effective June 10, 2026

Name:	Candice Robison
Position Title:	Legislative Coordinator & Executive Assistant
Department:	Legislative Services
Contact Email:	crobison@lethcounty.ca
Contact Phone:	403-380-1585

The Access and Privacy Advisor is responsible for:

- Ensuring the County's compliance with POPA and all associated regulations.
- Developing, implementing, and maintaining the Privacy Management Program and Corporate Directives.
- Acting as the primary point of contact for the Office of the Information and Privacy Commissioner.
- Overseeing privacy impact assessments, incident response, and employee training.
- Maintaining the Personal Information Inventory, PIA Registry, and AI and Automated Systems Register.

Signed: _____ Date: June 10, 2026

Chief Administrative Officer, Lethbridge County

Personal Information Inventory Template

Maintain one row per distinct personal information holding or program. Update whenever a program changes or a new system is introduced. Reviewed annually by the Access and Privacy Advisor.

Program / System	Info Type Held	Purpose	Legal Authority (POPA section)	Classification Level	Storage Location	Retention Period	Disposal Method
Payroll & HR Administration	Employee name, SIN, home address, banking details, benefits enrolment	Administer payroll, benefits, and employment records	POPA, Section 4(c)	Confidential	County HR/payroll system (access-controlled)	7 years after end of employment	Secure deletion / cross-cut shredding
Utility & Tax Billing & Accounts Receivable	Ratepayer/ account holder name, mailing and service address, billing and payment history, pre-authorized-debit banking details	Administer utility accounts, all taxes, and accounts receivable billing and collections	POPA, Section 4(c)	Confidential	County financial system	10 years	Secure deletion
Fire Services — Burn & Fireworks Permits	Applicant name, contact details, property location / legal land description	Issue and track burn and fireworks permits in support of fire safety	POPA, Section 4(c)	Internal / Confidential	Permitting / records management system	Current season plus 2 years (per records retention schedule)	Secure deletion
Planning, Development & Building Permits	Applicant name, contact details, property location, supporting documents	Process planning, development, and building/safety-codes permit applications	POPA, Section 4(c)	Protected / Internal	Permitting / records management system	Per records retention schedule (life of asset + statutory period)	Secure deletion / archival per schedule

Delegation of Authority Matrix

This matrix provides a summary-level overview of delegated POPA authority at Lethbridge County. The full legally operative delegation tables with specific section references are set out in LS01, Schedules A and B. The CAO retains all POPA authority unless expressly delegated in writing.

POPA Function	CAO / Head	Delegated Head	Access and Privacy Advisor
Approve PMP and Corporate Directives	Authority	Review and recommend	Develop and maintain
Designate Access and Privacy Advisor	Authority		
Respond to access requests	Authority	Oversight	Delegated — see LS01 Sched. B
Respond to correction requests	Authority	Oversight	Delegated — see LS01 Sched. B
Approve and submit PIAs to OIPC	Authority	Oversight	Delegated — see LS01 Sched. B
Respond to privacy complaints	Authority	Oversight	Delegated — see LS01 Sched. B
Manage privacy incidents and notifications	Authority	Oversight	Delegated — see LS01 Sched. B
Establish consent rules (oral, electronic)	Authority — established in LS02		
Authorize disclosure to avert imminent danger	Authority		Delegated — see LS01 Sched. B
Delegate powers, duties, or functions (POPA s.55)	Authority only — cannot be sub-delegated		

Corporate Directives Cross-Reference

The following table maps each POPA/M-Reg requirement to the governing Corporate Directive. This table is intended to assist employees and auditors in locating the applicable binding instrument for any specific obligation.

POPA / M-Reg Requirement	Section Reference	Governing Directive
Designation of Privacy Officer	M-Reg s.6(1)(a)	LS01, s.6.3; LS05, s.6.1
Delegation of authority (ATIA and POPA)	ATIA s.87; POPA s.55	LS01, Schedules A and B
Access to personal information	POPA Part 4	LS02, s.7.1
Correction of personal information	POPA s.7	LS02, s.7.2
Privacy complaints	M-Reg s.6(1)(b)(iii)	LS02, s.7.3
Consent — oral, written, electronic	Privacy Reg s.2; M-Reg s.6(2)(d)	LS02, s.7.4
Privacy incident response and notification	POPA s.10; M-Reg s.4	LS03, s.7.1
Privacy Impact Assessments	POPA s.26; M-Reg s.7	LS03, s.7.2–7.3
Proactive monitoring of information systems	M-Reg s.6(2)(c)	LS03, s.7.3.4
Non-personal data and data matching	POPA s.17–24; M-Reg s.5	LS04, s.7.1
AI and automated systems	M-Reg s.6(1)(b)(v), s.6(2)(f)	LS04, s.7.2
Human oversight of data-creating systems	Privacy Reg s.3(2)	LS04, s.7.1.6
Security classification system	M-Reg s.6(1)(d)	LS05, s.7.1
Mandatory employee training	M-Reg s.6(1)(f)	LS05, s.7.2
Administrative safeguards	Privacy Reg s.1(c); M-Reg s.6(1)(e)	LS05, s.7.3
Physical safeguards	Privacy Reg s.1(c); M-Reg s.6(1)(e)	LS05, s.7.4
Technical safeguards	Privacy Reg s.1(c); M-Reg s.6(1)(e)	LS05, s.7.5
PMP public availability	POPA s.25	This PMP, Section 17
PMP review cycle	M-Reg s.6(1)(g)	This PMP, Section 16
Personal information inventory	M-Reg s.6(1)(c)	This PMP, Section 8; Appendix B

Approved by:	_____ Chief Administrative Officer, Lethbridge County
Date:	_____
Next Review Date:	June 11, 2027 (annual review — see Section 16)