## ADM-39 Privacy Management Program

**Department: Administration**

### 1. Scope

#### 1.1 Purpose

1.1.1 The County has enacted this Privacy Management Program (PMP) in accordance with the requirements of section 25 of the *Protection of Privacy Act (POPA)* and section 6 of the *Protection of Privacy (Ministerial) R*egulations (PMR).

1.1.2 As a public body with custody or control of a high volume of personal information and highly sensitive personal information, this Privacy Management Program includes the prescribed requirements in both sections 6(1) and 6(2) of the PMR.

1.1.3 The goal of this Privacy Management Program is to promote the County's compliance with its duties under the POPA and PMR in a manner that is proportional to the volume and sensitivity of the personal information in the custody or under the control of the County.

1.1.4 Specifically, the purpose of this PMP is to:

a. Promote accountability within the County for the collection, use, disclosure, and protection of personal information and other privacy related matters.

b. Demonstrate the County's commitment to privacy and the proper administration of personal information.

c. Outline the safeguards and policies in place to protect personal information and to proactively identify and mitigate privacy risks.

d. Integrate privacy considerations in to the operations and planning of the County.

#### 1.2 Application

1.2.1 This Privacy Management Programs applies to all the personal information in the custody or under the control of the County, including the County's collection, use, disclosure, retention and deletion, and protection of that personal information.

1.2.2 This Privacy Management Program applies to all Council members and employees, as defined by the POPA, including any third party that performs a service for the County under contract.

## 2. Definitions

2.1.1 In this Privacy Management Program:

a. "**Artificial Intelligence or AI"** means any machine-based system that infers from the input it receives how to generate outputs, including predictions, content, recommendations, or decisions.

b. **"ATIA"** means the Access to Information Act, SA 2024, c A-1.4, as amended or replaced.

c. **"Automated system"** means any system, software, or process that uses computation as whole or part of a system to determine outcomes, make or aid decisions, inform policy implementation, collect data or observations, or interact with individuals. Automated systems include machine learning, statistics, or other data processing or artificial intelligence systems, but excludes passive computing.

e. **"Employee"** means an employee of the County and includes a person who performs a service for the County as an appointee, volunteer or student or under a contract or agency relationship with the County.

d. **"Highly sensitive personal information"** means information that is considered highly sensitive in accordance with section 1 of the PMR, including biometric or financial information, or personal information about a minor, senior, or vulnerable individual.

e. **"OIPC"** means the Office of the Information and Privacy Commissioner of Alberta.

f. **"Personal information"** means recorded information about an identifiable individual, as defined by the POPA.

g. **"PIA"** means a privacy impact assessment, as defined by section 26 of the POPA and section 7 of the PMR.

h. **"PMP"** means Privacy Management Program as defined by section 25 of the POPA and section 6 of the PMR.

i. **"PMR"** means the *Protection of Privacy (Ministerial) Regulations*, Alta Reg 143/2025, as amended or replaced.

j. **"POPA"** means the *Protection of Privacy Act*, SA 2024, c P-28.5, as amended or replaced.

k. **"PPR"** means the *Protection of Privacy Regulations*, Alta Reg 132/2025, as amended or replaced.

l. **"Privacy complaint"** means a complaint from an individual that their personal information has been collected, used, or disclosed in contravention of the POPA.

m. **"Privacy Head"** means the individual designated as the head of the County pursuant to section 1(i) of the POPA and section 3.1 of this PMP, or their delegate.

n. **"Privacy incident"** or **"privacy breach"** means any loss of, unauthorized access to, or unauthorized disclosure of personal information in the custody and under the control of the County.

o. **"Project"** in relation to a PIA, means an administrative practice, program, project or service.

p. **"Public Body"** or **"the County"** means the County St. Paul No. 19.

2.1.2 This PMP further adopts the defined terms of the ATIA and POPA, and their associated regulations. To the extent there is any conflict between a defined term in this PMP and any Act or Regulation, the definition in the Act or Regulation shall prevail.

## 3. Roles and Responsibilities under the POPA

### 3.1 Privacy head of the Public Body

3.1.1 In accordance with section 1(i) of the POPA and sections 1(h)(iii) and 98(a) of the ATIA, the Privacy Head of the County for the purposes of the POPA is the individual who holds the position of Chief Administrative Officer within the County as per Bylaw 2023-17

3.1.2 The Privacy Head of the County may delegate any authority under the POPA to another employee of the County in accordance with section 55 of the Act. If the Privacy Head of the County has delegated their authority under the POPA, that delegation is to be recorded in Appendix C to this PMP.

3.1.3 The Privacy Head of the County is accountable for the County's overall performance and compliance with the POPA and is responsible for carrying out the powers, duties, and functions of the Privacy Head as specified in the POPA.

### 3.2 Privacy Officer

3.2.1 The County is required by section 6(1)(a) of the PMR to designate a Privacy Officer who is responsible for ensuring the County's compliance with the POPA.

3.2.2 The Privacy Officer for the County is designated to be the individual who holds the position of ATIA Coordinator within the County.

3.2.3 In accordance with this PMP and any other relevant policies and procedures of the County, the purpose of the role of Privacy Officer is to:

a. Serve as the primary contact within the County for privacy matters, including privacy incidents and complaints, and requests for corrections to personal information.

b. Support the creation, development, and review of privacy policies and procedures.

c. Ensure the County is operating in a manner that is compliant with POPA and this PMP.

d. Facilitating employee training and education on privacy matters.

e. Representing the County during matters before the OIPC.

f. Liaising with third parties, such as service provides, insurers, technical specialists, and legal counsel on privacy matters.

### 3.3 Privacy Management Structure

3.3.1 Where applicable, the Privacy Officer shall report directly to the Privacy Head of the County, or their delegate, in respect of any matter falling within the scope of the POPA or this PMP.

3.3.2 Any employee of the County who has a matter involving compliance with this PMP or the POPA shall report the matter to the Privacy Officer, or their direct supervisor who shall then report the matter to the Privacy Officer.

3.3.3 All employees, Council members, service providers, and volunteers of the County are responsible for complying with privacy obligations under this PMP or the POPA, including completing mandatory privacy training.

### 3.4 Collection of Personal Information

3.4.1 The County will only collect personal information where it has a valid purpose of the collection of that personal information in accordance with section 4 of the POPA.

3.4.2 The County will only collect personal information in a manner provided for in section 5(1) of the POPA.

3.4.3 Where the County collects personal information directly from an individual, the County will provide notice to the individual in accordance with sections 5(2) and 5(4) of the POPA at the time of the collection.

3.4.4 Notice in accordance with section 5(2) of the POPA must be provided for the collection of personal information in oral, written, electronic, video, or audio formats.

3.4.5 The Privacy Officer may establish a standard collection notice to be used by the County in accordance with section 5(2) of the POPA, which will then be referenced in Appendix D to this PMP.

3.4.6 Changes to the standard collection notice may be made on an as-needed basis in consultation with the Privacy Officer.

### 3.5 Use of Personal Information

3.5.1 The County is prohibited from selling personal information for any purpose.

3.5.2 The County will only use personal information in a manner provided for in section 12(1) of the POPA.

3.5.3 The County will use personal information only to the extent necessary to enable the County to carry out the purpose of the use in a reasonable manner.

### 3.6 Disclosure of Personal Information

3.6.1 The County will only disclose personal information where provided for in section 13(1) of the POPA.

3.6.2 The County will only disclose personal information to the extent necessary to enable the County to carry out the purpose for disclosure in a reasonable manner.

## 4. Privacy Policies and Procedures

4.1.1 The County is required by section 6(1)(b) of the PMR to establish and identify certain policies and procedures that address the County's duties under the POPA, including:

a. Corrections to personal information [section 5 of this PMP];

b. Privacy incident response [section 6 of this PMP];

c. Privacy complaints response [section 7 of this PMP];

d. The creation, use, and disclosure of non-personal data [section 9 of this PMP];

e. The use of personal information with respect to automated systems and artificial intelligence [section 10 of this PMP];

4.1.2 Policies and procedures of the County that involve the County's collection, use, disclosure, retention or destruction, or protection of personal information, or otherwise engage a power, duty, or function of the County under the POPA, should be made with reference to this PMP to ensure consistency and compliance of privacy measures and policies across the County.

4.1.3 The County will maintain a list of policies and procedures that involve the collection, use, disclosure, retention or destruction, or protection of personal information, or otherwise engage a duty or responsibility of the County under the POPA, as Appendix A to this PMP.

## 5. Corrections of personal information

### 5.1 How to request corrections

5.1.1 In accordance with section 7 of the POPA, individuals may request the County correct their personal information if the individual believes there is an error or omission in their personal information that is in the custody or under the control of the County.

5.1.2 Individuals may make requests to correct their personal information in writing to the Privacy Head or their delegate by email. The Privacy Head or their delegate is responsible for determining whether the correction should be made in accordance with the POPA.

5.1.3 The Privacy Head or their delegate cannot correct opinions about an individual, including professional and expert opinions. Corrections are to be made to factual statements of personal information [e.g. a birth date].

5.1.4 If the Privacy Head or their delegate does not correct the information, for any reason, an annotation or link must be made with the personal information that was requested to be corrected with the requested correction so long as the requested correction is relevant and material to the record containing the personal information.

### 5.2 Notice of Corrections, Annotations, Linkages

5.2.1 The Privacy Head or their delegate must make the decision to correct the personal information and notify the individual of their decision within 30 business days of the request being made. The individual must be notified that either a correction was made, or an annotation or linkage was made.

5.2.2 The Privacy Head or their delegate may apply to the Information and Privacy Commissioner for an extension to the 30-business day period.

5.2.3 Where the County has corrected the personal information, or annotated or linked the personal information, the Privacy Head or their delegate will notify any other public body or third party who the County has disclosed the personal information to in the year before the correction request was made.

5.2.4 Notice under this section must state that either a correction was made, or if no correction was made that an annotation or linkage was made.

5.2.5 In accordance with section 7(5) of the POPA, the Privacy Head or their delegate does not need to provide notice where it is the Privacy Head's or their delegate's opinion that the correction, annotation, or linkage is not material and the individual who made the requested correction agrees in writing that the notification is not necessary.

5.2.6 If the County receives notice from another public body that a correction, annotation, or linkage has been made, the Privacy Head or their delegate must make the correction, annotation, or linkage on any record containing the personal information included in the notice that is in the County's custody or under its control.

### 5.3 Transferring correction requests

5.3.1 If the County receives a request to correct personal information, and the personal information was collected by another public body or another public body created the record containing the personal information that is the subject of the correction request, the Privacy Head or their delegate may transfer the correction request to the other public body.

5.3.2 A transfer of a request to correct personal information must be done within 15 business days of the date it was received.

5.3.3 If the Privacy Head or their delegate transfers the request, the County must notify the individual who made the correction request as soon as possible.

5.3.4 If a request to correct personal information is transferred to the County, the Privacy Head or their delegate must make reasonable efforts to respond to the request within 30 business days after receiving the transferred request.

## 6. Privacy Incidents

### 6.1 Identification, investigation, and escalation

6.1.1 If the County experiences, or is suspected to have experienced, a privacy incident or breach, the individual who discovers or suspects the incident or breach must immediately report it to the Privacy Officer, or to their direct supervisor who must immediately report it to the Privacy Officer.

6.1.2 The Privacy Officer, in coordination with other employees of the County as necessary [e.g. IT, human resources, or internal legal counsel], shall take immediate steps to investigate, stop, contain, or mitigate the privacy incident.

6.1.3 The Privacy Officer will as soon as reasonably possible report the privacy incident to the Privacy Head.

6.1.4 The Privacy Officer may also report the privacy incident to, and coordinate the County's response to the incident with, external stakeholders as necessary, including third-party service providers [e.g. external cybersecurity or IT providers, communications advisors], the County's insurer, and/or external legal counsel (as necessary).

### 6.2 Real Risk of Significant Harm

6.2.1 Once the privacy incident has been stopped or contained, the Privacy Officer – in coordination with other employees of the County as necessary – shall make the following determinations:

a. What personal information was the subject of the privacy incident;

b. Whether the loss, unauthorized access or disclosure of the personal information identified in (a) constitutes a significant harm to the individuals who the personal information is about, in accordance with section 4(2) of the PMR;

c. Whether as a result of the privacy incident, there exists a real risk of that significant harm to an individual, in accordance with section 4(1) of the PMR.

6.2.2 In making the determination as to whether a privacy incident has resulted in a real risk of significant harm to an individual, the Privacy Officer may consult the Office of the Information and Privacy Commissioner's guidance on breach notification and the POPA Breach Notice Assessment Tool.[1]

### 6.3 Notice of a Privacy Incident

6.3.1 If the Privacy Officer determines that there exists a real risk of significant harm to an individual as a result of the privacy incident, the Privacy Officer shall ensure the County gives notice as required by section 10(2) of the POPA.

6.3.2 The form and content of the notice given to an individual for who there exists a real risk of significant harm as a result of the privacy incident shall comply with section 4(3) of the PMR.

a. Notice given under this section should follow the template notice set out in Appendix E of this PMP.

[1] https://oipc.ab.ca/breach-notification/

6.3.3 The form and content of the notice given to the Information and Privacy Commissioner shall comply with section 4(4) of the PMR.

a. The County shall give notice to the Information and Privacy Commissioner using the Office of the Information and Privacy Commissioner's breach notification form.[2]

6.3.4 The form and content of the notice given to the Minister shall comply with section 4(5) of the PMR.

a. The County shall give notice to the Minister using the Government of Alberta's online reporting portal.[3]

6.3.5 The notices required by section 10(2) of the POPA are to be given without unreasonable delay, having regard to the nature and context of the privacy breach, the actions required to stop, contain, and mitigate the breach, and the assessment of the real risk of significant harm to the affected individuals.

### 6.4 Documenting Privacy Incidents

6.4.1 The Privacy Officer should document a privacy incident concurrent to the steps taken under the other provisions of this section of the PMP to assist the County in assessing and documenting the nature and scope of the incident, the steps taken to stop, contain, or mitigate the incident, if there is a real risk of significant harm as a result of the incident, whether notice is required to be given in accordance with the POPA, when and how that notice is given, measures put in place to prevent future incidents, or how the County's incident response may be improved.

6.4.2 In documenting a privacy incident, the Privacy Officer should use the Privacy Incident Report template included in Appendix F of this PMP.

[2] Available at https://oipc.ab.ca/breach-notification/.
[3] https://www.alberta.ca/report-a-privacy-incident-public-bodies

## 7. Privacy Complaints

### 7.1 Receiving a complaint

7.1.1 Individuals may make privacy complaint to the County by submitting such a complaint, in writing, to the Privacy Officer.

7.1.2 The Privacy Officer may contact the complainant to request any additional information necessary for the County to investigate or resolve the privacy complaint.

### 7.2 Investigation and resolution

7.2.1 Upon receipt of a privacy complaint, the Privacy Officer may investigate a complaint. The Privacy Officer may choose not to investigate a complaint in situations where, including but not limited to:

a. The privacy complaint is abusive, threatening, frivolous, or vexatious.

b. There is insufficient information provided by the complainant to investigate the privacy complaint.

7.2.2 Regardless of whether or not the County conducts an investigation into the privacy complaint, the Privacy Officer may decide whether to respond to a complainant or not.

7.2.3 If the Privacy Officer decides to respond to the complainant, the response may state that:

a. the County has decided not to investigate the complaint;

b. the County investigated the complaint and determined there was no unauthorized collection, use, or disclosure of the complainant's personal information; or

c. the County investigated the complaint and determined there was an unauthorized collection, use, or disclosure of the complainant's personal information, and any resolution or mitigative measures proposed or implemented by the County.

7.2.4 If the Privacy Officer decides to respond to a complainant, the response must be given within 30 business days of the day the privacy complaint was received as required by section 38(2) of the POPA.

7.2.5 Nothing in this section of this PMP is intended to alter any process set out in the POPA or any steps that the County may or is required to take in response to a request or direction from the Information and Privacy Commissioner.

## 8. Privacy Impact Assessments

### 8.1 What is a PIA and when are they required?

8.1.1 A Privacy Impact Assessment (PIA) is a process that assists the County in reviewing the impact that a new project or significant change to an existing project may have on individual privacy. The purpose of a PIA is to:

a. Identify and review risks associated with the County's collection, use, and disclosure of personal information under the new or changed project.

b. Develop mitigation strategies and safeguards regarding those risks.

c. Address how the County will comply with its duties under the POPA.

d. Document the identification and mitigation of privacy issues on a proactive basis.

8.1.2 Privacy Impact Assessments must be completed by the County when the County is implementing a new, or a substantial change to an existing, project that will involve the collection, use, or disclosure of personal information, and if one of the following criteria – as set out in section 7(1) and 7(5) of the PMR – are met:

a. The personal information at issue, if the subject of a privacy incident, could result in significant harm to an individual.

b. The project will collect, use, or disclose highly sensitive personal information.

c. The project will involve the personal information of a significant percentage of the population served by the County.

d. The project will involve data matching between the County and another public body.

e. The project is part of a common or integrated program or service.[4]

f. The project involves the development or use of innovative technology, including an automated system and artificial intelligence.

8.1.3 In addition to the legislated requirements of the POPA and PMR, the County may use the PIA Assessment Tool from the OIPC to assist it in determining whether a PIA is required for a project.[5]

### 8.2 Who completes the PIA and when?

8.2.1 It is the responsibility of all employees of the County to identify when the County is implementing a new or substantial change to an existing project that involves the collection, use, and disclosure of personal information, such that a PIA may be required and notify the Privacy Officer that a PIA may be required.

8.2.2 The Privacy Officer will make the determination as to whether a PIA is required or should otherwise be completed.

8.2.3 The PIA will be completed by the Privacy Officer in coordination with the manager or director of the County that is responsible for the implementation of the new, or substantial change to the existing, project.

[4] See section 1(d) of the POPA for the definition of "common or integrated program or service."
[5] https://oipc.ab.ca/wp-content/uploads/2025/06/PIA_Submission_Assessment_Tool_202506.pdf

### 8.3 Completing a PIA

8.3.1 When completing a PIA, the County must include all of the required content as set out in section 7(2) of the PMR, including:

a. A summary of the purpose of the collection, use, or disclosure of personal information for the new, or a substantial change to an existing, project.

b. Identification of the personal information that will collected, used, or disclosed, and the security arrangements that will be put in place to protect that personal information.

c. Identification of the legal authority under the POPA or other legislation for the collection, use, or disclosure of the personal information.

d. Identification of the privacy risks associate with the collection, use, or disclosure of personal information, and how those risks may be mitigated.

e. Identification of the safeguards, as discussed in section 12 of this PMP, in place to protect the personal information, including when the personal information is transmitted, matched, or linked.

f. Describe how the County will ensure the personal information is accurate and complete, how corrections to the personal information will be handled, and how the information will be retained.

g. The governance structure between the County and another public body over the personal information if the project is part of a common or integrated program or service.

8.3.2 Where the County has previously prepared a PIA for a project, the PIA may be amended or updated to account for any substantial change in fulfillment of the requirements of the POPA.

8.3.3 To complete a PIA, the County will use the PIA Template provided by the OIPC as the standard form for all PIAs, in recognition that the OIPC requires a public body to follow that template if the PIA is required to be submitted to the Information and Privacy Commissioner. In addition, the County may use the OIPC's PIA Template Completion Guide for guidance when completing a PIA.[6]

8.3.4 A PIA must include a level of detail consistent with the complexity of the project that the PIA relates to. For instance, if the PIA relates to the implementation of an automated system or artificial intelligence the PIA may also include an algorithm impact assessment.[7]

### 8.4 Submitting a PIA to the OIPC

8.4.1 The County is required to submit a copy of a PIA to the OIPC where required to do so by section 7(5) of the PMR.

8.4.2 Specifically, if the reason for the PIA being completed is one of the criteria in section 8.1.2(b) to (f) of this PMP,[8] then the PIA must be submitted to the OIPC in accordance with the PMR.

---

[6] The PIA template and template completion guide are available at: https://oipc.ab.ca/resource/popa-pia-template-completion-guide/
[7] See Appendix C of the OIPC's template completion guide (link above).
[8] See also section 7(5) of the PMR.

## 9. Data derived from personal information and non-personal data

### 9.1 Definitions

9.1.1 For the purposes of this PMP:

a. "Data-derived from personal information" – as defined in the POPA – means data created by data matching and that identifies any individual whose personal information was used in the data matching.

b. "Data matching" – as defined in the POPA – linking personal information between two or more databases or other electronic sources of information.

c. "Non-personal data" – as defined in the POPA – means data, including data derived from personal information, that has been generated, modified, or anonymized so that it does not identify any individual and includes synthetic data and any other type of non-personal data identified in the regulations to the POPA.

d. "Synthetic data" – as defined in the POPA – means artificial data created to maintain the structure and patterns of real data without being linked to any individual in the original data set.

### 9.2 Data matching

9.2.1 The County in carrying out data matching may only:

a. Do so for a purpose as set out in section 17(1) of the POPA.

b. Collect personal information in accordance with section 17(2) of the POPA.

c. Retain and use data derived from personal information in accordance with section 18 of the POPA.

d. Disclose data derived from personal information in accordance with section 19(1) of the POPA.

9.2.2 The County must protect any data derived from personal information in accordance with section 20 of the POPA.

### 9.3 Non-personal data

9.3.1 The County in creating non-personal data may only:

a. Do so for a purpose as set out in section 21(1) of the POPA;

b. Create non-personal data in accordance with sections 21(2), (3), and (4) of the POPA.

c. Use non-personal data in accordance with section 22 of the POPA.

d. Disclose non-personal data in accordance with section 23 of the POPA.

9.3.2 Before creating any non-personal data, the County will establish a data quality assurance process in accordance with section 5(1) of the PMR.

9.3.3 Before using or disclosing any non-personal data, the County will conduct an assessment as specified in section 5(2) of the PMR.

9.3.4 The County must protect any non-personal data in accordance with section 20 of the POPA.

## 10. Automated systems and artificial intelligence

### 10.1 The use of automated systems

10.1.1 The County may use dedicated automated systems, automated systems integrated into the County's information technology or productivity software, or artificial intelligence tools to assist in providing an operating program or activity of the County, as permitted by the Privacy Head.

10.1.2 Employees and Council members are prohibited from using personal automated system, including artificial intelligence tools, accounts as part of their duties or roles with the County, unless they receive authorization from the Privacy Head.

10.1.3 In allowing the use of automated systems or AI tools provided by the County or providing authorization under section 10.1.2, the Privacy Head may specify conditions, in addition to the requirements of this PMP, to the use of those automated systems or AI tools by employees and Council members, including:

a. What purpose an automated system or AI may be used for.

b. What types of information, including personal information, may be used as an input or prompt into an automated system or AI.

c. How the output of an automated system or AI may be used by the employee or Council member, and what degree of human oversight is required.

d. What security measures are required before an automated system or AI can be used with personal information.

10.1.4 The County may at any time implement a standalone automated system or artificial intelligence policy, which may replace or alter this section of the PMP.

### 10.2 Personal information and automated systems

10.2.1 Notwithstanding any written condition provided under this section, the County, including its Council members and employees, shall not input any personal information into an automated system or AI tool without having provided notice to the individual(s) whose personal information is being inputted that their personal information is being inputted into an automated system or AI to generate content or make decisions, recommendations, or predictions in accordance with section 5(2) of the POPA.

10.2.2 The requirement to provide notice, as set out above, includes when an automated system or AI is being used to record or transcribe a call or meeting with any individual, including employees of the County, where personal information may be discussed.

10.2.3 Where personal information is inputted into an automated system or AI, the output generated by the automated system or AI tool must be reviewed, including to verify the accuracy of the personal inputted into or outputted by the automated system, by the employee or Council member who inputted the personal information prior to any further use or disclosure of that output.

10.2.4 The output generated by an automated system or AI is not to be used as the sole basis for any decision where personal information was an input into the automated system or AI, or where the decision affects an individual. The automated system's output must be verified or confirmed by the appropriate decision maker within the County prior to any decision being made.

10.2.5 The County will keep a record of any decision made where an automated system or AI is used to assist in making a decision in accordance with section 10.2.4, including what personal information was inputted into the automated system or AI tool, the output of the automated system or AI tool, and how the output was used by the decision maker in making a final determination.

## 11. Security classification

### 11.1 Security classification requirements

11.1.1 The County is required by section 6(1)(c) of the PMR to establish a security classification system for any personal information, data derived from personal information, and non-personal data in the custody or under the control of the County.

11.1.2 The purpose of the security classification system is to ensure the right security arrangements and safeguards are in place to protect personal information based on the type or sensitivity of the personal information and protect against the risk of loss or unauthorized access, use, disclosure of the personal information and any harm that may result.

11.1.3 The security classification system must 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 County, which must reflect the sensitivity of the personal information.

11.1.4 The security arrangements, administrative safeguards, physical safeguards, and technical safeguards established by the County to protect for personal information data derived from personal information, or non-personal data must be proportional to the security classification level of the personal information or data.

### 11.2 Security classification system

11.2.1 The County has developed the following security classification system to apply to all personal information in its custody or under its control:

11.2.2 The County has developed the following security classification system to apply to all types of information, including personal information, in its custody or under its control:

| Level | Definition | Examples |
|---|---|---|
| Public | Information that is available to the public, including on the external website, or is otherwise available on request. | Council minutes and public agendas, annual budgets and financial reporting, bylaws, policies. |
| | Personal information or data that if lost, accessed, used or disclosed without authorization would not result in harm to an individual or the County. | Employee names and positions, published news or media reports, information posted to County's website. |
| | | Personal information that if disclosed would not be an unreasonable invasion of personal privacy as defined by section 20 of the ATIA. |

| | | |
|---|---|---|
| Internal | Information that is widely available to employees of the County, but is not readily available to the public. | Internal business records, except for those classified as restricted. |
| Confidential | Personal information or data that if lost, accessed, used or disclosed without authorization would result in harm to an individual or the County. | Personal information such as contact information, race, ethnic origin, religion, nationality, age, gender identity, sex, marital or family status, educational or employment history. |
| Restricted | Information that is only available to certain employees or departments within the County and information that is not to be made public unless required by law.<br><br>Personal information or data that if lost, accessed, used or disclosed without authorization would result in serious harm to an individual or the County. | Personal information such as biometric information, health information, financial information, educational, financial, criminal history, highly sensitive personal information.<br><br>Information that is subject to legal privilege or required to be kept confidential by law or contract. Workplace investigations. |

11.2.3 The examples provided are not determinative of the security classification level for any piece or type of information. The determination of the security classification level to be applied to a piece or type of information is to be made by the employee creating the record containing the information based on the definitions provided and the considerations of the information and individual to whom it belongs. If necessary, the Privacy Officer may be consulted on the application of the security classification levels.

11.2.4 Nothing in this security classification system affects any obligation or right the County may have to use or disclose information, data derived from information or data under the POPA, the ATIA, or any other statute or law.

11.2.5 For the purposes of this section, “harm” is to be defined as including, but not limited to, the types of harms set out in section 4(2) the PMR. For clarity, the classification level of information is not determinative of whether there exists a real risk of significant harm should that information be subject to a loss, or unauthorized access or disclosure.

### 11.3 Implementation

11.3.1 Information in the custody or under the control of the County must be classified in accordance with this security classification system, including records containing information that are created, used, or disclosed entirely within the County, as well as

records containing information that are created, used, or disclosed to persons external to the County.

11.3.2 Classification of a record is to be based on the information within the record that has the highest potential for harm. For example: an internal memo with information classified as Public and Confidential is to be given the classification of Confidential; an email sent to a third-party service provider with predominantly Confidential personal information with limited excerpts of Restricted information, is to be given the classification of Restricted.

11.3.3 All records created by the County after the date that this PMP comes into force should be marked with the classification level assigned to the information within the record.

## 12. Monitoring of Personal Information, Security Arrangements, and Safeguards

### 12.1 Proactive monitoring of personal information

12.1.1 The County may establish processes for the proactive monitoring of information systems that hold or store personal information, including based on the security classification level of the personal information within the system or the potential harm posed by the loss, unauthorized access, or unauthorized disclosure of the personal information.

12.1.2 The Privacy Head or the Privacy Officer may complete periodic reviews or audits of access to personal information controls or may otherwise monitor the collection, use, disclosure, storage, retention, or destruction of personal information or information systems.

12.1.3 Proactive monitoring may include automated monitoring, regular inspections by employees, or random or irregular inspections by employees of information systems.

### 12.2 Security arrangements

12.2.1 The County will maintain or implement reasonable security arrangements to protect personal information, data derived from personal information, and non-personal data against risks including that of unauthorized access, collection, use, disclosure, or destruction.

12.2.2 The security arrangements for a piece or type of personal information will be appropriate and proportional with the security classification level of that personal information.

12.2.3 Security arrangements, as defined in the PPR, include:

a. Administrative safeguards;

b. Physical safeguards;

c. Technical safeguards.

12.2.4 The following table is to be used as a guide for the County in establishing security arrangements and safeguards for personal information in accordance with the security classification level.

| Level | Safeguards |
|---|---|
| Public | Administrative: subject to the County's record management bylaw, policies, and associated schedules on records retention; may be accessed by employees of the County; review before disclosure by employee responsible for operating program or activity; disclosure confirmed to be in accordance with POPA or ATIA; standard privacy training for employees.<br>Physical: Regular storage in the County's offices or information and document management systems.<br>Technical: standard information system security measures, including ensuring software and security patches are up-to-date and reviewed regularly. |

| | |
|---|---|
| Internal | Administrative: Public Safeguards;[9] controls to limit access to employees who require personal information for performance of duties; review of information before disclosure by employee responsible for operating program or activity with consult to Privacy Officer, if necessary; confidentiality provisions in contracts.<br>Physical: Public Safeguards.<br>Technical: Public Safeguards; encryption or password protected where necessary. |
| Restricted | Administrative: Public Safeguards; strict controls to limit access to limited number of employees based on role and employee level; review before disclosure by manager/director and Privacy Officer; confidentiality provisions in contracts; consult with legal counsel prior to access, use disclosure, if necessary.<br>Physical: Secure and locked storage in the County's offices with limited employee access.<br>Technical: Public Safeguards; encryption and multi-factor authentication; electronic controls or permissions required for access by employees; password protection when disclosed. |

12.2.5 In addition to the specified safeguards, the County will ensure that all administrative, physical, and technical safeguards are updated regularly, including by reviewing policies, employee access permissions, ensuring software and security patches are current.

[9] Where indicated, the safeguards for a security classification level should include, at a minimum, the safeguards for the lesser security classification level (e.g. the administrative safeguards for Confidential personal information should include the administrative safeguards for Public personal information, in addition to or as altered by the safeguards specific to Confidential personal information.

## 13. Obtaining consent

### 13.1 When consent is required

13.1.1 In accordance with the POPA, the County does not require consent to collect personal information; however, notice is required when collection is from the individual whose personal information is being collected. Consent is sufficient to allow the County to use or disclose personal information in accordance with sections 12 and 13 of the POPA, respectively.

13.1.2 The PMR requires that the County establish procedures related to managing consent under the POPA.

### 13.2 Obtaining consent

13.2.1 For clarity, where an individual has provided consent and the County seeks to rely on that consent in accordance with sections 12 and 13 of the POPA, that consent must meet the requirements of section 2 of the PPR, including:

a. That it meets the requirements for written, electronic, or oral consent specified in the PPR;

b. That it specify the personal information to which the consent relates;

c. That it specify how the personal information may be used or to whom the personal information may be disclosed.

d. That it specify the date on which the consent is effective, and if applicable, the date on which the consent expires.

13.2.2 Where written, electronic, or oral consent is being provided in accordance with the POPA and this PMP, the County may require an individual to provide identification prior to accepting their consent as the basis to use or disclose their personal information.

13.2.3 Consent may be withdrawn on notice to the County, after which the consent will no longer be valid under the POPA. If an individual seeks to withdraw their consent, the County may inform the individual the effect that withdrawing their consent may have on the County's ability to use or disclose their personal information.

### 13.3 Electronic Consent

13.3.1 The Privacy Head has determined that the County will accept electronic consent for any purpose that it would accept written consent. If an individual is expected to or asks to provide electronic consent, the County will explicitly communicate that electronic consent is acceptable.

13.3.2 The County will accept the following forms of electronic consent and signature:

a. Electronic signatures attached through dedicated pdf signing software (e.g. Docusign);

b. An electronic signature file or image inserted into a document or email that appears next to the individual's name;

c. Where the individual inserts "signed electronically" next to their name in a document or email.

d. Any other standard permitted by the Privacy Head where it is clear the individual has created or adopted an electronic signature for the purpose of providing consent

### 13.4 Oral Consent

13.4.1 The Privacy Head has determined that the County will accept oral consent for any purpose that it would accept written consent, but only where the personal information being used or disclosed is classified as either Public or Confidential. Oral consent will not be accepted by the County for personal information classified as Restricted. The County will explicitly confirm with an individual whether oral consent is to be accepted.

13.4.2 Where the County accepts and obtains oral consent, the County will ensure a record of the consent is retained in accordance with the requirements of section 5(d) of the PPR.

13.4.3 Where the County accepts and obtains oral consent, the County will take any steps necessary to verify the identity of the individual providing the consent.

## 14. Privacy Training

### 14.1 Mandatory training for employees

14.1.1 As required by section 6(1)(d) of the PMR, it is mandatory for employees of the County to receive training regarding the County's and its employee's obligations under the POPA.

14.1.2 Mandatory training is required for any employee, Council member, or volunteer of the County that is involved in the collection, use, disclosure, or protection of personal information as part of their employment, officer or volunteer duties with the County.

14.1.3 In addition to the mandatory training specified above, the County may require or provide additional privacy training to employees or Council members who are regularly involved in the collection, use, disclosure, or protection of high volumes of personal information, highly sensitive personal information, or whose roles or duties would benefit from such training.

14.1.4 The mandatory training for new employees will be provided by the County within three months of their start of their employment.

14.1.5 The mandatory training for existing employees will be provided within six months of the enactment of this PMP, and then at least every two years after an employee last received training.

## 15. Availability and Review of PMP

### 15.1 Availability of PMP

15.1.1 The County will make this PMP available via its website.

15.1.2 In accordance with section 6(4) of the PMR, the County may withhold technical information, security-related information and other information that could compromise the security of personal information in the custody or under the control of the County from the publicly available version of this PMP.

### 15.2 Review of PMP

15.2.1 This PMP shall be reviewed and assessed, and updated if necessary, within 2 years of its enactment and then every at least every 3 years thereafter.

Council Approved: June 9, 2026

**Appendix A – List of Associated Policies and Procedures**

**The following are policies and procedures of the County that fall within the scope of section 4 of this PMP:**

- County of St. Paul No. 19 Records Retention and Disposition By-law, as amended or replaced, and associated schedules.
- County of St. Paul No. 19 Records Retention & Disposition Policy ADM-39.
- Access to Information and Protection of Privacy Policy ADM-36.

**Appendix B – Legislation Reference Table**

| Section of this PMP | Section of POPA, PPR, PMR |
|---|---|
| Section 1 | Section 25 of the POPA |
| Section 2 | Section 1 of the POPA<br>Section 1 of the PMR |
| Section 3.1 | Section 1(i) of the POPA [and sections 1(h)(iii) and 98(a) of the ATIA] |
| Section 3.2 | Section 6(1)(a) of the PMR |
| Section 3.3 | Section 6(2)(a) of the PMR |
| Section 3.4 | Sections 4 and 5 of the POPA |
| Section 3.5 | Sections 11, 12(1), and 12(4) of the POPA |
| Section 3.6 | Section 13(1) and 13(4) of the POPA |
| Section 4 | Section 6(1)(b) of the PMR |
| Section 5.1 | Section 7(1) and (2) of the POPA<br>Section 6(1)(b)(i)(A) of the PMR |
| Section 5.2 | Section 7(3) to (7) of the POPA |
| Section 5.3 | Section 8 of the POPA |
| Section 6.1 | Section 6(1)(b)(i)(B) of the PMR |
| Section 6.2 | Sections 4(1) and 4(2) of the PMR |
| Section 6.3 | Section 10(2) of the PMR<br>Sections 4(3) to 4(5) of the PMR. |
| Section 7.1 | Section 6(1)(b)(i)(C) of the PMR |
| Section 7.2 | Section 38(2) and 38(3) of the POPA |
| Section 8.1 | Section 26 of the POPA<br>Section 6(2)(a)(ii) and 7(1) and 7(5) of the PMR |
| Section 8.2 | Section 7(1) of the PMR |
| Section 8.3 | Section 7(2) of the PMR |
| Section 9.1 | Section 1 of the POPA |
| Section 9.2 | Sections 17, 18, 19, and 20 of the POPA |
| Section 9.3 | Sections 20, 21, 22, and 23 of the POPA<br>Section 5(2) and 6(1)(b)(ii) of the PMR |
| Section 10.1 | Sections 6(1)(b)(iii) and 6(2)(a)(v) of the PMR |
| Section 10.2 | Section 5(2) of the POPA |
| Section 11.1 | Sections 2 and 6(1)(c) of the PMR |
| Section 12.1 | Section 6(2)(a)(iii) of the PMR |
| Section 12.2 | Section 10(1) of the POPA<br>Sections 1(1)(c) and 1(2) of the PPR<br>Sections 3 and 6(2)(b) of the PMR |
| Section 13.1 | Sections 12(1)(b) and 13(1)(c) of the POPA<br>Section 6(2)(a)(iv) of the PMR |
| Section 14 | Section 6(1)(d) of the PMR |
| Section 15.1 | Sections 6(3) and 6(4) of the PMR |
| Section 15.2 | Section 6(1)(e) of the PMR |

**Appendix C – Delegation of Authority**

In accordance with section 55(1) of the POPA, the Privacy Head of the County has hereby delegated the following powers, duties, or functions under the POPA to stated individuals:

| **Authority/Section of POPA** | **Delegated Head of County** |
|---|---|
| Sections 5(3) and 5(4) – dispensing with collection notice | ATIA Coordinator |
| Sections 7 and 8 – corrections of personal information | ATIA Coordinator, Payroll Technician, Taxation and Assessment Technician |
| Section 13(1)(s), (cc), (ee) – disclosure of personal information | ATIA Coordinator |
| Section 15 – disclosure for research and statistical purposes | ATIA Coordinator |
| Section 23 – disclosure and conditions for non-personal data | ATIA Coordinator |
| Sections 28, 39, and 41 – advice and representations to the Information and Privacy Commissioner | ATIA Coordinator |
| Section 44 – duty to comply with Commissioner's orders | ATIA Coordinator |
| Section 54(1)(e) – determination of rights to be exercised on behalf of a minor | ATIA Coordinator |

**Appendix D – Sample Collection Notice**

**[Section 5(2) of the POPA]**

**Purpose of sample collection notice**

In instances where the County is collecting personal information directly from an individual and is required by section 5(2) of the POPA to provide notice at the time of collection of:

a. the purpose for which the information is collected,
b. the specific legal authority for the collection,
c. the email address, telephone number or other contact information to which the individual may direct the individual's questions about the collection, and
d. the public body's intention, if any, at that time to input the information into an automated system to generate content or make decisions, recommendations or predictions;

the County may use or adapt this standard collection notice. Prior to the County implementing this collection notice for a specific collection of personal information, the Privacy Officer will review the notice and its proposed use to confirm it is accurate and adequate for the specific collection of personal information (e.g. inclusion on an intake form).

**Notice of Collection of Personal Information**

*The County is collecting your personal information, including* ***[insert specific personal information being collected if possible]*** *under the authority of section 4* ***[insert specific subsection of section 4 – most often it may be 4(c), but 4(b) applies in terms of law enforcement matters. If 4(a) is relied on then the specific provision of the other enactment should be referenced as well]*** *of Alberta's Protection of Privacy Act. This information will be used by the County for the purpose of* ***[insert general description of purpose of collection]****.*

**[IF APPLICABLE]** *The personal information collected may be inputted into automated systems or artificial intelligence tools to [insert general description of use of automated system or AI tool, such as generate a summary, recommendation, etc.] as part of the County's purpose for collecting your personal information. All decisions made based on the personal information provided are made by an employee of the County.*

*The County may use and disclose your personal information where permitted or required to by law, including where permitted by the Access to Information Act or Protection of Privacy Act.*

*If you have any questions about the collection of your personal information, you may contact the County's Privacy Officer.*

**Appendix E – Sample Privacy Incident Notice**

**[Section 4(3) of the PMR]**

**Notice of Loss, Unauthorized Disclosure, and Unauthorized Access of Personal Information**

In accordance with the County's obligations under the *Protection of Privacy Act* and the *Protection of Privacy Ministerial Regulations*, the County is writing to provide notice that your personal information that was in the custody and under the control of the County was subject to **[a loss – an unauthorized disclosure – an unauthorized disclosure]**.

The personal information that was subject to the **[loss – unauthorized disclosure – unauthorized disclosure]** includes:

- [Insert list of personal information affected, e.g. name, contact information, employment history (start date, salary (if not public). It does not have to be a finite list of every piece of personal information, but needs to be a general description so the individual understands what information was affected].

On [**insert date of discovery of privacy incident**], the County became aware that the personal information described above was [**insert description of circumstances of the loss, unauthorized access to, or unauthorized disclosure of personal information as required by section 4(3)(ii) of the PMR** – for example, "was accessed by unauthorized third party who gained access to the County's servers" or "was accidentality disclosed via email to …"]. The **[loss – unauthorized disclosure – unauthorized disclosure]** initially occurred on **[insert date of incident**].

After discovering and investigating the **[loss – unauthorized disclosure – unauthorized disclosure]** of your personal information, the County took the following steps to mitigate and reduce the risk of harm that may arise as a result of this incident:

- [Insert list of mitigating and harm reducing steps taken. These will be context specific and should be developed in consultation with all relevant stakeholders – cybersecurity providers, insurers, legal counsel].

If you have any questions regarding this notice, please contact the County's Privacy Officer at [insert privacy officer email].

The County takes its duty to protect personal information seriously and will take steps to prevent similar incidents from occurring in the future. In keeping with the County's obligations under the *Protect of Privacy Act* notice of this incident has also been given to the Information and Privacy Commissioner and the Minister of Technology and Innovation.

Under section 37 of the *Protection of Privacy Act* you have a right to ask the Information and Privacy Commissioner to review this incident. A request to the Commissioner to review the circumstances of this incident must be in writing, must give notice of the request to the County, and should contain sufficient detail, including a copy of this notice, to allow the Commissioner to review the incident. For more information on requesting reviews by the Commissioner, please see the Office of the Information and Privacy Commissioner's website for more information on requesting a review.

**Appendix F – Template Privacy Incident Report**

**Privacy Incident Report**

**Name of Privacy Officer completing privacy incident report:**

**Date report was started:**

**Date report was completed:**

**Section 1 – Description of Incident**

**Date and time privacy incident was discovered:**

**Date and time privacy incident first occurred:**

**Describe circumstance of incident** (including how the incident occurred, nature and scope of the incident, how the incident was discovered and by who):

**Section 2 – Affected personal information**

**Describe the types of personal information that were subject to loss, unauthorized access, or unauthorized disclosure as a result of the privacy incident:**

**Number of individuals whose personal information was subject to the privacy incident:**

**Names and contact information of individuals whose personal information was subject to the privacy incident [either list here or confirm information is available]:**

**Section 3 – Response and mitigation**

**Describe the steps taken by County upon discovery of privacy incident to report incident within the County [e.g. who within the County was notified of the incident and when, what immediate steps were taken to investigate, stop, contain, or mitigate the privacy incident]:**

**Describe the third-party stakeholders that were notified of the privacy incident in an effort to investigate, stop, contain, or mitigate the privacy incident [e.g. external cybersecurity or IT service provider, insurer, external legal counsel, external communications providers]:**

**Describe any other relevant information or investigative steps taken by the County or a third-party stakeholder to investigate, stop, contain, or mitigate the privacy incident:**

**Section 4 – Assessment of real risk of significant harm**

With reference to section 4 of the *Protection of Privacy Ministerial Regulations* and section 6.2 of the County's Privacy Management Program, the County is required to determine whether the personal information subject to the privacy incident presents a real risk of significant harm to any individual.

In making the determination as to whether a privacy incident has resulted in a real risk of significant harm to an individual, the Privacy Officer may consult the Office of the Information and Privacy Commissioner's guidance on breach notification and the POPA Breach Notice Assessment Tool.[10]

[10] https://oipc.ab.ca/breach-notification/

**Assessment of whether upon the affected personal information being lost, or disclosed or accessed with authorization there may be significant harm, as defined in section 4(2) of the *Protection of Privacy Ministerial Regulations* [list potential types of harm and how they would arise as a result of the incident]:**

**Assessment of whether there exists a real risk of the significant harms, as described above, to an individual as a result of the privacy incident:**

a. whether there is a reasonable basis to believe that the personal information has been misused or will be misused.

b. whether the loss of, unauthorized access to or unauthorized disclosure of the personal information occurred as a result of malicious intent.

c. the sensitivity of the personal information that was lost or accessed or disclosed without authorization.

d. mitigating measures taken or other factors that reduce the risk of significant harm.

e. any other relevant factors or considerations that may affect the assessment of whether there exists a real risk of significant harm.

**Summary of assessment of real risk of a significant harm** [the Privacy Officer must determine whether on consideration of the types of personal information affected, the harm that personal information could cause, and the potential for those harms to occur whether there is a real risk of significant harm]:

**Section 5 – Notification of privacy incident**

If the Privacy Officer has determined that there is a real risk of significant harm to an individual as a result of the privacy incident, notification must be given to the individual, the Information and Privacy Commissioner, and the Minister of Technology and Innovation.

See the County's Privacy Management Program for information on how to give notice to each of the individual, Commissioner, and Minister.

**Date notice given to individual(s):**

**Date notice given to Information and Privacy Commissioner:**

**Date notice given to Minister:**

**Section 6 – Lessons learned**

**Describe any steps or measures identified by the County in responding to this privacy incident that should be implemented by the County going forward to reduce the likelihood or the impact of future privacy incidents:**

**Describe whether any additional amount of privacy training for employees or Council members is required or recommended as a result of the privacy incident:**

**Review of Privacy Incident Report by Privacy Head**

**Date:**

**Signature of Privacy Head**