CITY OF ST. ALBERT

ADMINISTRATIVE PROCEDURE

TITLE		
Privacy, Access and Security Governance Procedures		
DEPARTMENT	**APPROVAL DATE**	**DATE LAST REVISED**
Legal, Legislative & Records Services	June 8, 2026	N/A

1. PURPOSE

To provide governance standards for the collection, use, disclosure, protection and access to personal information, data derived from personal information and non-personal data in accordance with **Privacy, Access and Security Administrative Directive A-LS-07**.

These procedures must be read in conjunction with the Administrative Directive. Where an inconsistency exists, the Directive prevails.

2. SCOPE

These procedures apply to:

All City employees including officers, contractors, students, and volunteers providing services on behalf of the City;

All recorded information, in whatever form or medium (paper, digital, audio-visual, graphic) created or received in the course of carrying out the City's mandated functions and activities; and

All facilities and equipment required to collect, manipulate, transport, transmit, or keep City information.

3. CONSENT STANDARDS

3.1. The City can only request the consent of the individual for use or disclosure of their personal information, not for collection.

3.2. Individual consents for use or disclosure of personal information must include:

a) the identity of the individual or authorized representative providing the consent;

b) the purpose for which the information is being disclosed and how it can be used;

c) the personal information to which the consent relates;

d) the identity of the third party to whom the information will be disclosed;

e) an acknowledgement that the individual providing the consent has been made aware of the reasons why the information is needed and the risks and benefits to the individual of consenting or refusing to consent;

f) the date the consent is effective and the date, if any, on which the consent expires;

g) a statement that the consent may be revoked at any time by the individual providing it; and

h) an attestation affirming the consent or revocation by the individual or authorized representative.

3.3. A consent or revocation of consent is authenticated by the signature of the individual providing consent. Signatures are in writing either manually or electronically.

3.4. Electronic signatures are considered valid only if the level of electronic authentication is sufficient to confirm the identity of the individual who is granting or revoking the consent.

3.5. Oral consent is not routinely accepted by the City. Should oral consent be implemented, the City will ensure the consent adheres to the requirements of the POPA Regulation, including a recording of the consent.

4. RESEARCH PROJECT AGREEMENTS

4.1. Researchers are required to submit a Research Proposal Form (Appendix 2) for consideration and approval by the PAC.

4.2. The City discloses personal information for research purposes only if the recipient signs a Reasearch Agreement Form (Appendix 3).

5. NON-PERSONAL DATA BEST PRACTICES AND REQUIREMENTS

5.1. The City will develop and implement best practices and standards and techniques:

a) to locate and remove direct and indirect identifiers in personal information to create non-personal data; and

b) to ensure to a reasonable standard that individuals cannot be re-identified within the non-personal data by unauthorized users.

5.2. When creating non-personal data, and before it is used or disclosed, the City will:

a) verify the effectiveness of methods used;

b) ensure that methods used can be replicated for audit purposes;

c) identify the occurrence and source of potential bias in the data; and

d) ensure accuracy and completeness of data if it is used to inform decisions about programs or services.

5.3. Whenever non-personal data is created from personal information under its custody or control, and before it is used the City will record and maintain in a register:

a) a description of the personal information or data derived from personal information used to create the non-personal data;

b) the purpose for creating the non-personal data;

c) the method used for creating the non-personal data;

d) the information security classification of the data; and

e) the assessment completed to ensure that the identity of the individual who is the subject of the non-personal data cannot be identified or re-identified from the data.

6. RIGHT OF ACCESS AND CORRECTION OF INFORMATION

6.1. Right of Access Intake

Requests to access information where there is clearly no requirement or allowance to withhold or sever any of the requested information are provided as soon as possible outside of the right of access process.

Requests for access to information from an individual applicant that may involve review and severing must be in writing to the City Privacy and Access Coordinator or designate. Oral applications are accepted if the applicant has a physical disability or if their command of English is limited. These special applications must be completed through the Privacy and Access Coordinator.

All requests for access to information or correction that require the formal process are directed to the Privacy and Access Coordinator for response, who formally acknowledges receipt of request.

Applicants making requests for information may be required to provide sufficient information to verify their identity and authorize access to the information. Any such information provided is used for these purposes only.

The Privacy and Access Coordinator acknowledges receipt of the request to the applicant and informs them of the process and the 30 business day timeline involved in responding to the request.

The Privacy and Access Coordinator will engage with applicants to ensure that the request provides enough clarity and detail to identify and locate the requested records within a reasonable amount of time and effort. If the Privacy and Access Coordinator requests further detail and clarification, the applicant must respond within 30 business days or the request will be considered abandoned.

Within 15 business days after the City receives a request, the Privacy and Access Coordinator may transfer the request and if necessary, the record to another public body

if the record was produced by or for the other public body, the other public body was the first to obtain the record or the record is in the custody or control of the other public body. The Privacy and Access Coordinator will notify the applicant of the transfer.

6.2. Fees

Information requested is identified as either “personal information” or “general information.” Fees for these services based on these designations are charged according to the Fee Schedule (Appendix 1).

There is no administration fee for applicants requesting access to their own personal information. However, fees may be charged for reproduction of information, if required, and only when the estimated costs exceed $10.00.

A $25.00 administration fee is charged for requests for general information and is non-refundable. Additional fees may be charged for reformatting, reproduction, disclosure preparation or transmission of information, only when the estimated costs exceed $150.00.

The Privacy and Access Coordinator creates an estimate of the fees and provides it to the applicant. The applicant must decide to either accept the estimated cost, to revise or cancel their application, or to request a waiver of all or part of the fees. The applicant must respond within 30 business days or the request will be considered abandoned.

If the applicant requests a waiver of fees, the Privacy and Access Coordinator may waive all or part of the fees if a) the applicant cannot afford the payment, b) the records relate to a matter of public interest, or c) for any other reason by which it is deemed fair and reasonable in this particular case. The Privacy and Access Coordinator responds to a request for waiver of fees within 30 business days.

The applicant is required to pay, if applicable, the $25.00 administrative fee and/or a deposit of 50% of the estimated fees before the records are processed. The request will not be processed until the initial required fees are paid.

Regardless of the fee estimate, the City only charges fees beyond the initial administrative fee that reflect the actual costs incurred.

6.3. Retrieval and Review of Relevant Records

After the request intake fee requirements have been met, the Privacy and Access Coordinator or designate identifies, retrieves and reviews the requested records to determine where mandatory or discretionary exceptions to the right of access apply.

The Privacy and Access Coordinator or designate identifies and initiates searches functions, business units, employees, and information repositories that may hold records relevant to the request.

The Privacy and Access Coordinator or designate reviews on a line-by-line basis and severs words or portions of the record according to the mandatory or discretionary exceptions to the right of access, including an assessment of whether the release of the information would be an unreasonable invasion of privacy (Appendix 4). The reviewer may consult with appropriate employees to determine the application of severing.

6.4. Third Party Reviews

If the Privacy and Access Coordinator decides that affected third parties need to be consulted to determine the application of mandatory exceptions, the third parties are identified and contacted as soon as practicable.

The notification to the third party provides:

a) a notice that a request has been made for information that would affect them as a third party;

b) a copy of the information; and

c) a request to advise the Privacy and Access Coordinator to either disclose the information or explain why the information should not be disclosed.

The third party must respond to the notification and request within 20 business days.

The Privacy and Access Coordinator also notifies the applicant that a third party has been notified and that a decision about the application of exceptions will be made within 30 business days from the date of notice to the third party.

When the Privacy and Access Coordinator decides on whether or not to disclose the information after consultation with a third party, both the applicant and third party are notified.

The third party may ask the Commissioner to review the decision to disclose the information within 20 business days after the notice of decision is submitted to the third party.

6.5. Response to Applicant

Having completed a review of the records, the Privacy and Access Coordinator ensures that information subject to any of the exceptions to access in the Act is severed from the record prior to the record being disclosed to the applicant, with annotations or explanations identifying which exception has been applied to the specific information severed.

The final response will include the requested records, an explanation for all information severed, and that the applicant has a right to review the decision to withhold information with the Information and Privacy Commissioner.

Requested information will be provided in a form that is generally understandable. The City will endeavor to explain the meaning of the content, codes and abbreviations included in the applicant's record to the extent that it is reasonably practical.

The final response with relevant records will not be released to the applicant until all outstanding fees are received, including the remaining 50% of the fee estimate adjusted to the actual costs incurred.

If applicants request to view original records in person, to preserve the integrity of the record and ensure that documents are not removed from the City, a designated Privacy and Access official will be present to supervise during the entire period of consultation.

6.6. Time limits for responding to a request

The City responds to right of access requests within 30 business days of the receipt of the request.

The 30 business day timeline is suspended from the time between submission of a fee estimate to the applicant and the applicant's acceptance of the estimate, amendment or the City's decision to waive of fees.

The response time may be extended for an additional 30 business days, if:

a) the applicant agrees to the extension; or

b) the volume of records is large and more time is needed to process the request; or

c) more time is needed to consult with a third party, another public body or another entity;

If the response time is extended, the Privacy and Access Coordinator notifies the applicant of the reasons for the extension, when a response can be expected, and that the applicant may make a complaint to the Commissioner about the extension.

The timelines are automated extended in:

a) third party reviews to accommodate time required to complete the process; and

b) an emergency, disaster or other unforeseen event that results in unplanned operation closure of interruption. In this case, the Privacy and Access Coordinator notifies the Commissioner as soon as possible of the operational closure, the anticipated re-opening, and when the re-opening occurs.

The Privacy and Access Coordinator may extend the date of response for an additional period of time, as required, for the same reasons.

6.7. Correction or Amendment Request Processes

Requests from individuals to correct / amend basic information about themselves (e.g. change of name or address) are handled as a routine correction of information, so long as the information is clearly limited to factual corrections that can be verified immediately.

The City employees take reasonable steps to verify the identity of the individual or authorized representative before processing the request. This may involve reviewing a driver's license or other identification.

Formal requests to correct or amend information subject to review must be in writing to the City Privacy and Access Coordinator. An individual may request the correction of another person's information only if they have that person's signed consent or they can prove they are the person's legal representative.

All formal requests for correction are directed to the Privacy and Access Coordinator for response, who formally acknowledges receipt of request.

The City responds to formal requests for correction of personal information within thirty (30) business days of receipt of the request.

If corrections or amendments are made, the original information is not deleted but retained and marked as incorrect, for example, by crossing out.

The City informs the applicant in writing of the refusal or acceptance of the request, the reason(s) for the refusal, and any recourse the individual may have to challenge the City's decision.

If the request for correction or amendment is refused, the City annotates the record with reference to the requested correction or amendment. This may be done by linking the record electronically to the annotation information.

The Privacy and Access Coordinator notifies other organizations or agencies to whom the information was disclosed that a correction has been made, or that an annotation has been filed, unless the correction is not reasonably expected to impact on the ongoing provision of services.

6.8. Individual Challenges to Request Responses

Individuals are encouraged to bring any concerns or issues concerning responses to requests and compliance with this procedure to the Privacy and Access Coordinator for discussion and mediation. Formal complaints regarding a request will be handled in accordance with the Complaint Resolution process. For all requests, applicants will be advised of their right to request a formal review of the access process and the records by the Office of the Information and Privacy Commissioner of Alberta. Requests for review by the regulator must be made within 60 business days of the release of the records.

7. COMPLAINT RESOLUTION

7.1. Receiving Submissions

The Privacy and Access Coordinator reviews the submitted complaint to establish if it is submitted under ATIA or POPA and assigns an internal file number using the Complaint Submission Form (Appendix 8):

a) if the complaint is submitted under ATIA, identify the associated access request number and the employee who processed the request.

b) if the complaint is submitted under POPA, identify, if necessary, the associated record(s), employee(s), department(s), information system(s), or events connected to the complaint.

c) if the scope or nature of the complaint is unclear, the Privacy and Access Coordinator will contact the complainant to clarify it.

7.2. Acknowledge Receipt of Submission

Respond to the complainant, acknowledging receipt of submission, and providing an estimated date of response that is 30 business days from the date received.

7.3. Investigation and Analysis

The Privacy and Access Coordinator determines the scope and nature of the complaint according to the parameters established in the Directive and records the investigation scope as part of the complaint investigation file.

Based on the context of the complaint, the Privacy and Access Coordinator will collect and review any records associated to the complaint event that may provide additional context or relevant information. Records that are reviewed as part of the investigation are logged and indexed as part of the complaint investigation file.

The Privacy and Access Coordinator will review the complaint with any employees associated with it. If more than one employee is associated with the complaint, the Privacy and Access Coordinator will engage each employee individually. Interviews will begin with the employee most closely involved in the event. Relevant factual information from the interviews may be recorded as part of the complaint investigation file.

The Privacy and Access Coordinator will analyze the information from the complaint, associated records, and any interviews conducted to determine the findings of the investigation. Findings are based on a balance of probabilities.

Record the findings and any related information that informs the findings as part of the complaint investigation file. If it is determined through the findings that remediation actions are required, document the steps that will be taken and the date those actions will be performed.

7.4. Final Response

When the findings of the investigation are determined, a final written response using the Complaint Response Letter (Appendix 9) will be provided to the complainant according to the parameters set out in the Directive.

If the findings include remediation actions, the actions that will be performed and a date of completion will be provided to the complainant as part of the findings in the written response.

7.5. Resolution

Depending on the investigation findings and any identified risks regarding the creation, collection, use, disclosure of personal information, data derived from personal information, and non-personal data, the Privacy and Access Coordinator may identify further administrative, technical and physical safeguards that can be implemented to modify or prevent future contraventions in City systems, processes, and employee behaviours. This may include employee or user training, introduction of additional security technology, or upgrade to facilities or infrastructure.

8. INFORMATION SECURITY

The information security provisions of POPA require the City to protect personal information, data derived from personal information, and non-personal data in its custody or control by making Reasonable Security Arrangements to protect against unauthorized access, collection, use, disclosure or destruction. These procedures outline administrative, technical and physical safeguards in place in the City to protect confidential information.

8.1. SAFEGUARDS

ADMINISTRATIVE SAFEGUARDS

The City ensures that Council policies, administrative directives and procedures to facilitate the safeguarding of confidential information in its custody or control are developed and maintained.

The need for confidentiality and security of personal information is addressed as part of the conditions of employment for the City employees, beginning with the recruitment stage, and included as part of contracts. All employees are aware of, and appropriately trained with regard to, directives and procedures for safeguarding information.

All City employees, volunteers, officers, and contracted personnel that collect, use, disclose or have access to confidential information as part of the performance of their duties for the City sign a Confidentiality Agreement available here: https://stalbert.ca/preboarding/

Utilizing a system of levelled access by role, only the least amount of information necessary for the intended purpose is used or disclosed, and only to employees with a need to know. If the intended purpose can be accomplished without use or disclosure of identifying information, then the information is made anonymous.

Before implementing proposed new administrative practices or information systems that will change or significantly affect the collection, use and disclosure of personal information, the City completes a Privacy Impact Assessment (PIA) that describes how the new initiative will affect privacy, and what measures the City will put in place to mitigate risks to privacy.

An agreement or contract is completed and signed between the City and all contracted service providers that require access to the information systems and assets of the City that requires that they meet or exceed the City privacy program standards, directives and procedures.

City employees and persons acting on behalf of the City report all detected violations and breaches of sensitive data and or personal information as soon as possible to the City's Privacy and Access Coordinator by email submission to atia@stalbert.ca. This enables the Coordinator to take corrective action to resolve the immediate problem and minimize the risk of future occurrence.

Personal information that was used to make a decision about an individual will be kept for at least one (1) year after the decision has been made. Retention periods are captured in the City's Records Classification and Retention Schedule.

PHYSICAL SAFEGUARDS

All the City records, both onsite and offsite, are held and stored in an organized, safe, and secure manner in accordance with information security standards and the City's RIM Program Directive A-LS-03.

Appropriate fire detection and extinguishing devices are in areas where personal information is stored.

The City's records are not accessible by unauthorized people. In areas where unauthorized people are present, measures will be taken to ensure that files are not left unattended or accessible.

Computers or monitors that are left unattended in reception areas or areas where personal information is processed are secured and logged off, either manually or by default timer.

All servers and equipment storing electronic personal information are secured by locked cabinets or rooms within the City when not under direct supervision by an employee of the City.

The City records or equipment holding records (e.g. laptop computers) may not be left unattended in a vehicle, even if the vehicle is locked.

Where practical visitors are given name tags or badges, and an employee accompanies visitors to private or semi-private areas, to ensure that only authorized individuals are present in secure areas.

Appropriate measures are taken to control the distribution of keys or pass codes, and to ensure they are returned or changed after employment or association with The City has ended.

Confidential information will be treated with sensitivity. Employees will take care when sharing confidential and personal information if conversations can be overheard or intercepted by unauthorized individuals.

Confidential, restricted, or sensitive information that is transmitted by mail or courier will be sealed, marked as confidential, and directed to the attention of the authorized recipient.

Printers that may be used to send or receive confidential information are in a secure area. Employees use the "private print" feature when possible.

Destruction of records and information is managed in accordance with the City's Records and Information Management Program Directive A-LS-03

All information will be deleted using secure data wiping techniques prior to disposal of electronic data storage devices (e.g. surplus computers, internal and external hard drives, diskettes, tapes, CD-ROMS, etc.), or the device(s) will be destroyed.

TECHNICAL SAFEGUARDS

Firewalls, intrusion detection software, or other technical means to protect internal the City networks carrying identifiable personal information is in place to prevent unauthorized use and malicious software.

Administrative Directives: A-ITS-404 - Access Management, A-ITS-201 - Information Security Management, A-ITS-204 - Acceptable Use Agreement and A-ITS-205 - Server and Network Physical Security apply to these procedures.

Access to data and application systems to personal information is limited by each employee's functional role and on a need-to-know basis.

Employees of the City access and use information systems under their assigned User account or ID. The use of another person's assigned User account or ID is prohibited. The assigned User account or ID restricts access to data and application systems to that information based on their functional roles and need to know.

Access to the City information systems is controlled and password protected. Passwords are kept confidential at all times. Passwords will be changed on a regular schedule. If a computer is left unattended, it will be protected against unauthorized access by manual or automated locking or logout requiring authentication to re-enter the system.

Two-factor authentication is implemented for access to confidential information based on information security classification and/or the availability of authentication features.

Limited or routine personal information (e.g., names and contact details) may be transmitted by e-mail or over the internet or external networks where appropriate. More sensitive personal information is not permitted to be sent by e-mail or transmitted over the internet or external networks without the use of appropriate security safeguards, such as authentication and encryption. E-mail messages must also contain a confidentiality notification.

To detect unauthorized access and prevent modification or misuse of user data in applications, systems may be monitored to ensure conformity to access policies and standards. Appropriate security controls, such as event logs, will be implemented and reviewed as required to support adequate proactive monitoring of access.

Where possible, the City does not use service providers, including cloud services, that require the storage of personal information outside of Canada.

Computer systems that hold critical or sensitive information will be backed up, at a minimum, daily. Backed up information is stored in a secure environment offsite. Information that is intended for long-term storage on electronic media (e.g. tape, DVD, disk) will be reviewed on an ongoing basis to ensure the data is retrievable, and to migrate the data to another storage medium if necessary.

The City limits the use of AI services and applications via administrative directives and technical protections. Staff are directed to use only preapproved AI services and applications, which have means to monitor and control use with personal information.

8.2. INFORMATION SECURITY CLASSIFICATIONS

Classification levels and assignment

Information is classified according to the degree of harm that may result from unauthorized access, loss, or modification. Information is classified with the following levels identified in the Information Security Classification and Standards Table (Appendix 5) as:

a) Restricted

b) Confidential

c) Internal

d) Public

9. PRIVACY BREACH RESPONSE

This section is accompanied by the City's **Confidential** Cyber Security Event Management Plan. The PAC and IT work in collaboration to ensure those procedures are followed concurrently with the steps outlined below. Updates to either workflow will be made as required.

STEP 1: IDENTIFYING AND REPORTING PRIVACY BREACH

IDENTIFICATION AND REPORTING

When a privacy breach is identified, report the incident to your manager and the PAC within the Step 1 timelines in the Privacy Breach Procedures Table (Appendix 6). If unable to determine the level of the privacy breach, contact the PAC immediately.

The PAC will open and document the privacy breach using the Privacy Breach Response Form (Appendix 7) and will document the initial facts of the privacy breach as much as possible within the timelines available:

a) Dates of privacy breach and report

b) Responsive actions taken so far

c) Nature of the privacy breach: unauthorized collection, use, disclosure, loss, loss of access, or modification

d) Custody and control of the information breached

e) Extent and scale: distribution, location and volume of information

f) Known causes and recipients

g) Employees, individuals and organizations involved

ASSIGNING RISK LEVEL

When a privacy breach has been discovered, determine the level of the incident according to Privacy Breach Procedures Table (Appendix 6). The highest level where any one of the classes and characteristics apply is the identified Level of the privacy breach.

Level 1 Low:

Internal (I) class information:
The recipients or causes of the privacy breach are internal (an employee or contracted service provider) or external (someone outside the City).

Confidential (C) class information:
The recipients or causes of the privacy breach are internal only and recipients of the breached information do not know or have a relationship with any of the subject individuals involved.

Confidential (C) class information:
The cause of the privacy breach does not appear to be intentional.

Level 2 High:

Confidential (C) class information:
The recipients or causes of the privacy breach are external, involving persons who are not employees or contracted service provider.

Confidential (C) class information:
The recipients or causes of the privacy breach are internal and recipients of the breached information likely know or have a relationship with subject individuals involved.

Confidential (C) class information:
The cause of the privacy breach appears to be intentional.

Restricted (R) class information
The recipients or causes of the privacy breach are internal (an employee or contracted service provider) or external (someone outside the City).

Level 3 Critical:

Restricted (R) class information
The recipients or causes of the privacy breach are external, involving persons who are not employees or contracted service providers.

STEP 2: CONTAINMENT AND FURTHER REPORTING

CONTAINING THE PRIVACY BREACH

At this stage, employees use all available means to ensure that the information in the custody of unauthorized parties is returned to the City and/or destroyed irrevocably. If the recipient is uncooperative, this may involve legal action.

REPORTING

Depending on the level and nature of the privacy breach, IT, the City leadership and the RCMP are informed.

STEP 3: NOTIFICATION

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER (OIPC) AND GOVERNMENT OF ALBERTA

The PAC informs the Office of the Information and Privacy Commissioner of Alberta of all Level 2 or 3 privacy breaches that involve personal information, using the OIPC online process and any process established by the Ministry of Technology and Innovation.

Level 1 privacy breaches are generally not considered severe enough to pose a real risk of Significant Harm to an individual. However, each incident will be reviewed to confirm this status.

NOTIFICATION OF SUBJECT INDIVIDUALS

The PAC will notify identified subject individuals affected by all Level 2 or 3 privacy breaches, subject to review by the PAC. Subject individuals affected by Level 1 will be notified if required by OIPC.

Notifications involving large numbers of subject individuals and/or individuals for which contact information is unavailable may require the use of public media.

STEP 4: INVESTIGATION

INVESTIGATION PROCESS

Establish and confirm:

a) Dates of privacy breach and report
b) Responsive actions taken so far
c) Nature of the privacy breach: unauthorized collection, use, disclosure, loss, loss of access, or modification
d) Custody and control of the information breached
e) Extent and scale: distribution, location and volume of information
f) Know causes and recipients
g) Employees, individuals and organizations involved

Investigations establish facts based on evidence collected in documentation and interviews. Timelines to complete the investigation follow the standards based on the level of the privacy breach in the Privacy Breach Procedures Table (Appendix 8).

FINDINGS

As the outcome of the investigation, PAC will report findings on the causes, continuing risks of the privacy breach and notification activities completed. Findings are based on a balance of probabilities determination.

REPORT DISTRIBUTION

If RCMP are investigating the privacy breach for criminal enforcement purposes, coordinate activities with officers involved.

Investigative reports are distributed to Leadership and IT, HR, OIPC and the RCMP as required. Subject Individuals are given a summary of the findings in accordance with the City's Collection, Use, Disclosure and Right of Access procedures.

STEP 5: REMEDIATION AND PREVENTION

REMEDIATION

Remediation may have been started when immediate efforts were made to contain the privacy breach. The investigative report will identify any further gaps or weaknesses in information security that directly or indirectly caused the privacy breach and recommend immediate measures to close the gaps. Implementation and effectiveness of the remediation needs to be tracked.

PREVENTION RECOMMENDATIONS

The investigative report will identify further administrative, technical and physical security measures that can be implemented to prevent such privacy breaches in the wider systems, processes and behaviours. This could include employee or user training, introduction of additional security technology, or upgrade of facilities.

10. COMPLIANCE

Non-compliance with the Privacy, Access and Security Administrative Directive A-LS-07 may result in corrective action per A-HRS-02.05 Corrective Actions Directive.

APPENDIX 1: FEE SCHEDULE

The following fees are the *maximum* amounts charged to applicants under **ATIA Regulation.** For requests for personal information of the applicant, only fees for items 3-6 may be charged.

1. For searching for, locating and retrieving a record	$6.75 per 1/4 hr.
2. For converting or reformatting records:	
(a) converting a record into a redactable format	$0.25 per page
(b) reformatting audiovisual files into a redactable format	Actual cost to public body up to $20.00 per 1/4 hr.
3. For producing a paper copy of a record:	
(a) photocopies and computer printouts:	
(i) black and white up to 8 1/2” x 14”	$0.25 per page
(ii) other formats	$0.50 per page
(b) from microfiche or microfilm	$0.50 per page
(c) plans and blueprints	Actual cost to public body
4. For producing a copy of a record by duplication of the following media:	
(a) microfiche and microfilm	Actual cost to public body
(b) computer disks	$5.00 per disk
(c) computer tapes	Actual cost to public body
(d) slides	$2.00 per slide
(e) audio and video tapes	Actual cost to public body
5. For producing a photographic copy (colour or black and white) printed on photographic paper from a negative, slide or digital image:	
(a) 4” x 6”	$3.00
(b) 5” x 7”	$6.00
(c) 8” x 10”	$10.00
(d) 11” x 14”	$20.00
(e) 16” x 20”	$30.00
6. For producing a copy of a record by any process or in any medium or format not listed above	Actual cost to public body
7. For preparing and handling a record for disclosure.	$6.75 per 1/4 hr.
8. For supervising the examination of a record	$6.75 per 1/4 hr.
9. For shipping a record or a copy of a record	Actual cost to public body

APPENDIX 2: RESEARCH PROPOSAL FORM

PROPOSAL

Access to Personal Information for Research or Statistical Purposes

1. Researcher

Lead Researcher Name	**Organization (if applicable)**	
Position within organization	**Academic Advisor (if student)**	
Lead Researcher Contact Information		
Address	**Email**	**Phone**

2. Research Project Description

Project Title		
Purpose and Objectives of the Project		
Records Requested containing Personal Information	**Identifying (Y or N)**	**De-identified (Y or N)**
Duration of Access *Expected period of time during which access to the personal information will be required.*		
Requirement for individually identifying personal information *Explain why identifying personal information is required to achieve the purposes and objectives of the project.*		
Data-matching *Explain if and how any personal information will be matched or linked with other data sets to create new information. If so, also explain how the data-matching a) is not harmful to subject individuals and b) is clearly in the public interest.*		
Other project members requiring access to personal information		
Records	**Name and Project Role**	

3. Privacy and Security

Applications/Platforms *List the major platforms and applications that will be used to store, transmit and process the personal information, including cloud storage and access. List information that will be in paper/microform format. Describe security measures used to secure applications or platforms against unauthorized disclosure or loss.*

Devices/Locations

List the types and number of electronic devices that will be used to access, store or process the personal information and any restrictions on where and how they will be used. Describe security measures used to secure devices against unauthorized disclosure or loss.

For paper formats, describe the location where the information will be stored and accessed and the measures in place to security the records within the location.

Administrative Directive and Procedures

Attach any privacy and security policies and procedures the research team will follow in handling and processing the personal information.

Additional Privacy and Security Measures

4. Data Minimization

De-identification

List how and when personally identifying records will be de-identified.

Records	Method	Date

Describe measures used to ensure that de-identified information cannot be re-identified by reference or linkage to other available data sources. If re-identification needs to be maintained for the purposes of the research, what are the measures in place to prevent unauthorized re-identification.

Return and/or Destruction of Information

List how and when information will be returned to public body and/or irrevocably destroyed

Records	Return or Destruction	Method	Date

5. Attestation and Approval

By signing this proposal, the Lead Researcher affirms that the information submitted is, to the best of their knowledge, accurate and complete.

Signature of Lead Researcher	Date
Public Body Review and Approval	
Privacy and Access Coordinator Signature	**Date**
Functional Area Representatives Signatures *Representatives from functional areas who manage the identified records*	**Date**

APPENDIX 3: RESEARCH AGREEMENT FORM

AGREEMENT

Access to Personal Information for Research or Statistical Purposes

BETWEEN:

St. Albert (Organization)

AND

[Name of Researcher] (Researcher)

The Researcher agrees to following terms and conditions for accessing personal information based on the standards and descriptions set out in the approved Research Proposal attached as Schedule A.

1. Research Proposal

a) Personal information will be used only for the identified research purposes.

b) Access to the personal information will be restricted to project members listed.

2. Privacy and Security Conditions

a) The Researcher will comply with the *Protection of Privacy Act* (Alberta) and the Organization's privacy and security policies and procedures.

b) Personal information will be stored and used in a secure location and under secure conditions, as indicated.

c) Individual identifiers in the personal information will be removed or destroyed by the specified date.

d) The Researcher will not contact individuals to whom the personal information relates, directly or indirectly, without the prior written authority of the Organization.

e) No personal information will be used or disclosed by the Researcher in a form in which the individual to whom it relates can be identified, without the prior written authority of the Organization.

3. Breach of Agreement

a) The Researcher will notify the Organization immediately and in writing if and when a condition set out in this agreement has been breached.

b) If the Researcher fails to meet the conditions of the agreement, the agreement may be immediately cancelled, and the Researcher may be guilty of an offence under relevant legislation.

4. Attestations

Name and Role

_____ _____

Signature Date

Signatures of other project members requiring access to personal information:

Name and Role

_____ _____

Signature Date

Name and Role

_____ _____

Signature Date

Name and Role

_____ _____

Signature Date

Name and Role

_____ _____

Signature Date

SCHEDULE A

Access to Personal Information for Research or Statistical Purposes Proposal (Approved)

APPENDIX 4: UNREASONABLE INVASION OF PRIVACY GUIDELINES

There are several major factors to consider when deciding whether disclosure of personal information to someone who is not the person who is the subject of the information is unreasonable.

Step 1: Confirm the personal information

First, make sure that the information you are reviewing is personal information of a third party according to the personal information definition.

Step 2: Not an unreasonable invasion of personal privacy

Second, determine whether disclosing the personal information is NOT an unreasonable invasion of privacy. This is the case for the following types of information:

- Business title, address, or telephone number of an individual;
- Opinions contained in work product;
- The City employee classification, salary range, responsibilities, discretionary benefits;
- Information released 25 years after the death of the individual;
- Details of a license, permit, discretionary benefit given by [PUBLIC BODY] to an individual.
- The following personal information, so long as the individual has not expressly requested otherwise:
    a. Enrolment in a school
    b. Attendance at public event related to [PUBLIC BODY]
    c. Receipt of honour or award from public body

Step 3: Presumed unreasonable invasion of personal privacy

Third, for all other personal information, determine when disclosure is otherwise presumed to be an unreasonable invasion of privacy, by record types that document information about the individual:

- Medical, psychiatric or psychological records;
- Law enforcement records;
- Income or social assistance eligibility;
- Employment or educational history;
- Personal tax, banking or credit card details;
- Personal/personnel evaluations or recommendations, references;
- Names with other personal information, or on its own if it reveals identifiable personal, information; or
- Racial, ethnic, religious or political details.

Step 4: Other factors to consider

Fourth, if it helps to confirm your decision to disclose or not disclose the personal information, take into account the following considerations:

1. These factors would weigh in favour of disclosing personal information:
    a) advances public scrutiny;

b) promotes public health and safety or the protection of the environment;

c) provides a fair determination of the applicant's rights; or

d) assists in researching or validating claims, disputes or grievances of aboriginal people.

2. These would weigh in favour of withholding the personal information:

a) the third party is exposed unfairly to financial or other harm;

b) the personal information was supplied in confidence;

c) the personal information is likely inaccurate or unreliable; or

d) the disclosure would unfairly damage the reputation of any individual.

Step 5: Disclosure allowance

Finally, check to determine if POPA allows the City to disclose the personal information for the specific allowable circumstances listing in the Disclosure of Personal Information section. If the circumstances are applicable to the case, you may or, in the case of an ATIA access request, you would be required to disclose the personal information.

APPENDIX 5: INFORMATION SECURITY CLASSIFICATION AND STANDARDS TABLE

Class	Harm	Information Type
Restricted R	• Harm to operations of facilities or security systems • Immediate harm to health and safety of the public, clients, or employees • Loss of source record and accountability	• Information describing security systems, access codes, etc. • Personal or other information that would likely cause or allow a person to harm themselves or specific employees, or clients • Back-up of essential records
Confidential C	• Humiliation, damage to reputation • Identity theft • Financial or asset loss • Credit loss • Loss of employment, business or professional opportunity Harm to privacy of the public and employees • Economic loss for St. Albert or third parties • Damage to St. Albert credibility or service integrity • Legislative sanctions • Loss of source record and accountability	• All personal and employee information, including highly sensitive personal information • Data derived from personal information • Information given in confidence or under privilege • Third party business information • Deliberations, investigations, advice, decisions • Security audit tools • Non-personal data that has not been assessed and verified.
Internal Use I	Loss of source record and accountability	• Employee circulars (memos, everybody emails, Vine posts) • Administrative records available to public upon request, e.g., completed decisions, directives, reports • Source records of public information
Public P	No identified harms	• Published materials such as pamphlets, newsletter, annual reports • Public information such as directories or web sites • Non-personal data in aggregate or statistical form, in a report, summary or other publication, that has been assessed and verified

APPENDIX 6: PRIVACY BREACH RESPONSE PROCEDURES TABLE

Level	Severity Criteria		Time from Detection	Response	Responsibility
	Class	Characteristics (if any apply)			
1 Low	Internal and Confidential Class Information	Use this level when the breach involves **Internal** information, whether the cause or recipient is inside or outside the City. Also use this level when the breach involves **Confidential** information and all of the following are true: • the recipient or cause is **internal only**, • the recipient does **not know** and does not have a relationship with the affected individual(s), and • the breach does **not appear intentional**.	2 hours	*Step 1:* Report to Manager, and to PAC	Employee or Service Provider
			24 hours	*Step 2:* 1) Confirm privacy breach status 2) Contain privacy breach and retrieve information if possible 3) If the privacy breach is the result of an IT incident or involves an IT system follow these processes. If the privacy breach is the result of a cyber security breach the PAC and IT will also follow the cyber security processes. In all instances, inform the IT helpdesk and IT leadership. 4) Confirm requirement for notifications to OIPC, GoA, and subject individual(s)	PAC, Employee or Service Provider, IT, HR
				Step 3: If required: 1) Notify OIPC, GoA 2) Notify subject individual(s)	PAC
			20 days	*Step 4:* Investigate Investigative report to: 1) Leadership, if directed by the PAC 2) IT, via the IT helpdesk if applicable 3) HR, if applicable	PAC, Employee or Service Provider, Manager, IT
			TBD	*Step 5:* Remediation and Prevention	PAC, Employee or Service Provider, Leadership, IT, HR

Level	Severity Criteria		Time from Detection	Response	Responsibility
	Class	Characteristics (if any apply)			
2 High	Confidential and Restricted Class Information	Use this level when the breach involves **Confidential** information and **any one** of these applies: • the recipient or cause is **external**, • the recipient or cause is **internal** and the recipient likely **knows or has a relationship** with the affected individual(s), or • the breach **appears intentional**. Also use this level for **any breach of Restricted information** where the cause or recipient is internal or external.	1 hour	*Step 1:* Report to Manager, PAC	Employee or Service Provider
			3 hours	*Step 2:* 1) Confirm privacy breach status 2) Contain privacy breach and retrieve information if possible 3) If the privacy breach is the result of an IT incident or involves an IT system follow these processes. If the privacy breach is the result of a cyber security breach the PAC and IT will also follow the cyber security processes. In all instances, inform the IT helpdesk and IT leadership. 4) Inform Leadership, Communications 5) Inform RCMP on potential criminal or public safety concerns 6) Inform HR, if applicable	PAC, Leadership, Employee or Service Provider, IT, HR
			24 hours	*Step 3:* 1) Notify OIPC, GoA 2) Notify subject individual(s)	PAC
			7 days	*Step 4*: Investigate Investigative report to: 1) Leadership, Communications 2) IT, via the helpdesk if applicable 3) HR, if applicable 4) RCMP, if required 5) OIPC, if required 6) Subject individual(s) on basic findings (not full report)	Employee, Manager and PAC

Level	Severity Criteria		Time from Detection	Response	Responsibility
	Class	Characteristics (if any apply)			
			TBD	*Step 5:* Remediation and Prevention	PAC, Employee or Service Provider, Leadership, IT, HR
3 Critical	Restricted Class Information	Use this level when the breach involves **Restricted** information and the recipient or cause is **external** (someone who is not a City employee or contracted service provider).	Immediately	*Step 1:* Report to Manager, PAC	Employee or Service Provider
			1 hour	*Step 2*: 1) Confirm privacy breach status 2) Contain privacy breach and retrieve information if possible 3) Inform Leadership, Communications 4) If the privacy breach is the result of an IT incident or involves an IT system follow these processes. If the privacy breach is the result of a cyber security breach the PAC and IT will also follow the cyber security processes. In all instances, inform the IT helpdesk and IT leadership. 5) Inform RCMP on potential criminal or public safety concerns 6) Inform HR, if applicable 7) Inform high risk subject individual(s)	PAC, Leadership, Employee or Service Provider, IT, HR
			1 hour	*Step 3:* 1) Notify GoA, OIPC and consult with OIPC on response 2) Notify remaining subject individual(s)	PAC

Level	Severity Criteria		Time from Detection	Response	Responsibility
	Class	Characteristics (if any apply)			
			3 days	*Step 4*: Investigate/cooperate with RCMP and OIPC Investigative report to 1) Leadership, Communications 2) OIPC, if required 3) RCMP, if required 4) IT, via the IT helpdesk if applicable 5) HR, if applicable 6) Subject individual(s) on basic findings (not full report)	Employee, Manager and PAC
			TBD	*Step 5*: Remediation and Prevention	PAC, Employee or Service Provider, Leadership, IT, HR

APPENDIX 7: PRIVACY BREACH RESPONSE FORM

Privacy Breach Response

Privacy Breach #

1. IDENTIFCATION AND REPORTING

Breach began: _____ / _____ / _____ Time: _____AM/PM
MM / DD / YYYY

Breach ended: _____ / _____ / _____ Time: _____AM/PM
MM / DD / YYYY

Breach discovered: _____ / _____ / _____ Time: _____AM/PM
MM / DD / YYYY

Breach reported: _____ / _____ / _____ Time: _____AM/PM
MM / DD / YYYY

Reported by:

Name: _____ Position/Role:

Contact information:

Summary of privacy breach as reported

2. CONFIRMATION, CONTAINMENT

Privacy breach Level: Breach location:

Applicable Class and Privacy breach Characteristics:

Potential Harm:

☐ Physical harm to a person

☐ Humiliation or damage to reputation

☐ Financial

☐ ID theft, fraud

Other:

Additional information about privacy breach:
Content and volume of personal information breached:
Recipient name(s) and contact information:
Containment actions and dates:
☐ Contained: _____ / _____ / _____ Time: _____AM/PM MM / DD / YYYY ☐ Not contained
3. NOTIFICATIONS
Who has been informed of the incident?
☐ Information and Privacy Commissioner informed: _____ / _____ / _____ MM / DD / YYYY Consultation decision: Date: _____ / _____ / _____ MM / DD / YYYY ☐ Information and Privacy Commissioner not informed
Notification actions and dates:
☐ Notifications completed: _____ / _____ / _____ MM / DD / YYYY ☐ No notifications or incomplete actions:

4. INVESTIGATION		
Investigative actions and dates:		
Date	Individuals consulted/investigated and contact information	Role (subject, perpetrator, expert, witness)
Date	Documents/Data Consulted	
5. REPORT AND FOLLOW-UP		
Findings:		
Recommendations: Remediation: Prevention:		
Report distribution:		
		_____ / _____ / _____ MM / DD / YYYY
		_____ / _____ / _____ MM / DD / YYYY
		_____ / _____ / _____ MM / DD / YYYY
Follow up actions planned or executed		
		_____ / _____ / _____ MM / DD / YYYY
		_____ / _____ / _____ MM / DD / YYYY

	_____ / _____ / _____ MM / DD / YYYY

6. APPROVALS AND AUTHORIZATIONS

Name and signature of Investigator

_____ Date: _____ / _____ / _____
MM / DD / YYYY

Name and signature of applicable Leadership

_____ Date: _____ / _____ / _____
MM / DD / YYYY

_____ Date: _____ / _____ / _____
MM / DD / YYYY

Appendix 8: Complaint Submission Form

Privacy and Access Complaint Submission Form

PART A – COMPLAINT DESCRIPTION AND SUBMISSION

Please fill out the sections of the form below and return your completed form to the Privacy and Access Office of the City of St. Albert by [EMAIL] or [ADDRESS]. The Privacy and Access Office will acknowledge receipt of your submission and provide an estimated date of response in that acknowledgement.

Name	**Date**
Preferred Contact Method (Email or Phone Number)	
Is your complaint regarding an access to information (ATIA) request?	
☐ No ☐ Yes, please provide ATIA request number _____	
Please describe your complaint below. Include as much information as possible regarding the nature of your complaint. You may attach records to submit with this form if needed.	
Are you attaching any additional records with your form submission?	☐ No ☐ Yes

Privacy and Access Complaint Submission Form

PART B – ST. ALBERT INTAKE TO BE FILLED OUT BY THE PRIVACY AND ACCESS OFFICE

Date Received	**St. Albert File Number**
Date Acknowledgement Sent to Complainant	**Estimated date of response provided to Complainant (30 business days from date received)**
Complaint under ATIA or POPA	**Investigation Required?**
☐ POPA ☐ ATIA	☐ No ☐ Yes
Additional Information (ex. associated OIPC file number, other internal St. Albert references)	

Appendix 9: Complaint Response Letter

DATE]

[NAME]
[ADDRESS]

Dear [NAME]:

RE: [FILE NUMBER] [COMPLAINT TITLE]

This is to formally confirm our response to the above request submitted to us on [DATE COMPLAINT RECEIVED].

Your request was for the following information:

"[COMPLAINT SUBMITTED]."

- [LIST ANY DOCUMENTS RECEIVED WITH THE COMPLAINT].

We have reviewed the circumstances relevant to your request and have arrived at the following outcome:

[FINDINGS AND/OR STATEMENT OF JUSTIFICATION].

Our office is available to answer questions or provide some explanations once you have had a chance to review the material. Please contact me directly using the contact information contained at the end of this letter.

Under Part 3 of ATIA and Part 6 of POPA, you have a right to request a review of our response to your requests to the Office of the Information and Privacy Commissioner (OIPC) within 60 days of the receipt of this letter. You can submit a request for review by following the guidelines on the OIPC website at https://oipc.ab.ca/request-a-review-file-a-complaint/

The following is contact information for OIPC that will be helpful in making a request for review:

Office Hours

8:15 a.m. - 4:30 p.m. (Monday to Friday)
Closed during lunch hours and statutory holidays.

Phone and Email

Toll-Free: 1-888-878-4044
Edmonton office: (780) 422-6860

Calgary office: (403) 297-2728
Email: generalinfo@oipc.ab.ca

Mailing Addresses

Office of the Information and Privacy Commissioner (Edmonton)
#410, 9925 - 109 Street NW
Edmonton, AB T5K 2J8

Office of the Information and Privacy Commissioner (Calgary)
Suite 2460, 801 6 Avenue SW
Calgary, AB T2P 3W2

Sincerely,

[NAME]

Privacy and Information Coordinator, City of St. Albert

[OFFICE ADDRESS]

[PHONE NUMBER]