TROCHU
ALBERTA

PRIVACY MANAGEMENT PROGRAM:

- General Program Policy
- Privacy Policy
- Access Policy
- **SECURITY POLICY**

DRAFT DATE: July 13th, 2026

APPROVED:

Jamie M Collins

Table of Contents

INFORMATION SECURITY AND PRIVACY BREACH RESPONSE

POLICY # 2026-07-13-04

POLICY NAME: Trochu Privacy Management Program: Security Policy

Information Security and Privacy Breach Response

I. PURPOSE

The Town of Trochu ("Trochu") is bound by the requirements of the *Protection of Privacy Act* ("POPA"). The information security provisions of POPA require Trochu 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. POPA also requires Trochu to identify, respond to, and in some cases, report privacy breaches. This policy outlines administrative, technical and physical safeguards in place at Trochu to protect confidential information as well as Trochu's response to privacy breaches.

II. SCOPE

This policy applies to:

1. Trochu employees, including directors, officers, contractors, students, and volunteers providing services on behalf of Trochu;
2. All recorded information, in whatever form or medium (paper, digital, audio-visual, graphic) created or received in the course of carrying out Trochu's mandated functions and activities; and
3. All facilities and equipment required to collect, manipulate, transport, transmit, or keep Trochu information.

III. INFORMATION SECURITY

A. SAFEGUARDS

1. **ADMINISTRATIVE**:

a) Trochu ensures that policies and procedures to facilitate the safeguarding of confidential information in its custody or control are developed and maintained.

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

c) All Trochu employees, volunteers, directors, officers, and contracted personnel that collect, use, disclose or have access to confidential information as part of the performance of their duties for Trochu sign a Confidentiality Agreement.

d) 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.

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

f) An agreement or contract is completed and signed between Trochu and all contracted service providers that require access to the information systems and assets of Trochu that requires that they meet or exceed Trochu privacy program standards and policies.

g) Trochu employees and persons acting on behalf of Trochu report all violations and breaches of information security as soon as possible to Trochu's Privacy and Access Officer. This enables the Officer to take corrective action to resolve the immediate problem and minimize the risk of future occurrence.

h) The minimum retention period for records retention under ATIA and POPA is one (1) year. Personal information that was used to make a decision about an individual will be kept for at least one year after the decision has been made. Beyond that, the retention periods are set according to the business requirements, and applicable by-laws and schedules of Trochu.

2. **PHYSICAL**

a) All Trochu records, both on-site and off-site, are held and stored in an organized, safe, and secure manner in accordance with information security standards.

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

c) Trochu's records are not accessible by unauthorized persons. In areas where unauthorized persons are present, measures will be taken to ensure that files are not left unattended or accessible.

d) 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.

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

f) Whenever possible, Trochu records or equipment holding records (e.g. laptop computers) are not be left unattended in a vehicle. If records or equipment must be left in a vehicle, the vehicle must be locked.

g) An employee accompanies visitors to private or semi-private areas, to ensure that only authorized individuals are present in secure areas.

h) 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 Trochu has ended.

i) 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.

j) 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.

k) Trochu employees will verify the identity and credentials of courier services used for the transportation of personal information.

l) Fax machines and printers that may be used to send or receive confidential information are located in a secure area. All fax transmissions will be sent with a cover sheet that indicates the information being sent is confidential. Reasonable steps are taken to confirm that confidential information transmitted via fax is sent to a recipient with a secure fax machine.

m) All records retention and destruction at Trochu is in accordance with Bylaw 2026-05 Document Retention Bylaw.

n) 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.

3. **TECHNICAL**

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

b) Access to data and application systems containing personal information is limited by each Trochu employee's functional role and need to know. Access privileges to information repositories containing information classified as confidential, highly sensitive or restricted are reviewed periodically to ensure that access continues to match the employee's functions and status.

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

d) Access to Trochu information systems is controlled and password protected. Passwords are kept confidential at all times, and are not posted publicly, or shared with other employees. If a computer is left unattended, it will be protected against unauthorized access by manual or automated logout requiring authentication to re-enter the system.

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

f) 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 encryption and authentication.

g) 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.

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

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

B. INFORMATION SECURITY CLASSIFICATIONS

1. CLASSIFICATION LEVELS AND ASSIGNMENT

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

(i) Restricted

(i) Confidential

(ii) Internal

(iii) Public

2. Employees assign security classification to each repository, file or document as required. Records that are Restricted must be marked as such visibly in the presented record and included as part of the metadata of the record.

C. SECURITY IN CONTRACTING

1. Trochu ensures contracted service providers (e.g., contractors, consultants, support service providers or business partners) comply with Trochu's Privacy, Access and Security policies and procedures, or have equivalent policies in place.

2. If a contracted service provider requires access to personal information or system affecting the security of personal information as part of their services, they must sign a privacy and security agreement outlining the conditions of access (see Appendix 1), or have equivalent provisions within terms or use, licensing agreements or contract addendums.

3. Until a contract detailing explicit information security provisions has been executed, the contracted service provider is not given access to premises or systems containing confidential business or personal information of Trochu.
4. Information security provisions outlined in contracts with contracted service providers meet or exceed the standards set out in the Privacy, Access and Security policies and procedures. Any related contracted service provider i Privacy, Access and Security policies should be made available to Trochu upon request, including any updates or revisions that occur after execution of the contract.
5. All employees of contracted service providers who have exposure to and use Trochu information assets and systems sign a Confidentiality Agreement. Contracted service provider service providers should remind their employees on termination of their continued responsibility to maintain the confidentiality of Trochu information.
6. Contracted service providers immediately report breaches of confidentiality and privacy to the Trochu PAO.
7. Contracts with service providers that have access to Trochu information assets and systems include provisions that protect Trochu operations from circumstances where the information assets or systems may be compromised. In order to mitigate these situations, disaster recovery and system backup is included in all agreements, to a standard that meets or exceeds that of Trochu.
8. Contracts with service providers include provisions for destroying or returning all Trochu information assets, including hardware, system documentation and information assets upon termination of agreements and in accordance with contract provisions reflecting records retention and data management policy.
9. To ensure compliance with contracted provisions for information security, Trochu:
    a) Requests contractors sign an acknowledgement that they have received, read, and will comply with any Trochu privacy, access and security policies they are bound to follow under contract; and
    b) actively monitors contracted service providers with access to information assets or systems for inappropriate access or use and to ensure compliance with contract security provisions.
10. Trochu retains the right to inspect the premises and security practices of contracted service providers to ensure compliance with contract provisions and stated policies.
11. Trochu avoids using service providers that require the storage or transmission of personal information outside of Canada. If they are retained, Trochu ensures that they meet the same standards of security and compliance that are required of Canadian service providers, in order to fulfill POPA's requirement to prevent unauthorized collection, use, access, retention, destruction and disclosure of personal information.

IV. PRIVACY BREACH RESPONSE

A. POLICY

1. DEFINITION

a) A Privacy Breach (breach) is an unauthorized disclosure, use, destruction, loss, removal, or modification of information in the custody or control of Trochu. Events are considered unauthorized by reference to access, privacy and security policy and/or legislation. A breach may be accidental or the result of a deliberate act.

2. DETERMINING LEVEL OF RESPONSE

a) The severity of the breach determines the nature of the response reporting structure, remedial action, and the investigation process. In the response process, severity is based on:

(i) The security classification of the information, which takes into account potential and real harm to individuals and organizations;

(ii) The internal and external scope and scale of the breach;

(iii) The known relationship of the recipients to subject individuals; or

(iv) The intentionality of the cause.

b) Levels are determined when any of the designated classes and circumstances apply as indicated in Step 1 Identifying and Reporting Breach, which incorporates an assessment of the real risk of significant harm as a result of the breach.

3. INVESTIGATION PRINCIPLES

a) Trochu uses generally accepted investigative methods to obtain the most effective results while respecting the rights, privacy, and dignity of persons being investigated. Investigations will, as required, incorporate the following methodologies:

b) Keep investigation information confidential to protect the privacy of individuals investigated and to maintain the integrity of the investigation;

(i) Use surveillance or monitoring data to establish past or current actions on an as-needed basis;

(ii) Examine or confirm the veracity of facts or statements, sometimes using third party witnesses;

(iii) Inform participants of their status and the progress of the investigation as fully and quickly as possible so long as it does not jeopardize the integrity of the investigation;

(iv) Base findings and conclusions on balance of probabilities.

c) The breach investigation is an administrative rather than a disciplinary process. Once the report is delivered, it is the responsibility of Management and Human Resources to determine the appropriate disciplinary action.

B. PROCESSES

STEP 1: IDENTIFYING AND REPORTING BREACH

1. IDENTIFICATION AND REPORTING

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

b) The PAO will open and document the breach using the Privacy Breach Response Form and will document the initial facts of the breach as much as possible within the timelines available:

(i) Dates of breach and report

(ii) Responsive actions taken so far

(iii) Nature of the breach: unauthorized collection, use, disclosure, loss, loss of access, or modification

(iv) Custody and control of the information breached

(v) Extent and scale: distribution, location and volume of information

(vi) Known causes and recipients

(vii) Employees, individuals and organizations involved

2. ASSIGNING RISK LEVEL

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

(i) Level 1 Low:

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

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

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

(ii) Level 2 High:

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

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

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

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

(iii) Level 3 Critical:

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

STEP 2: CONTAINMENT AND FURTHER REPORTING

1. CONTAINING THE BREACH

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

2. REPORTING

a) Depending on the level and nature of the breach, IT, Trochu leadership and the police are informed.

STEP 3: NOTIFICATION

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

a) The Town of Trochu informs the OIPC of all Level 2 or 3 breaches that involve personal information, using the OIPC online process and any process established by the Ministry of Technology and Innovation.

b) Level 1 breaches are generally not considered severe enough to pose a real risk of significant harm. However, each incident will be reviewed to confirm this status.

2. NOTIFICATION OF SUBJECT INDIVIDUALS

a) Trochu will notify identified subject individuals affected by all Level 2 or 3 breaches. Subject individuals affected by Level 1 will be notified if required by OIPC.

b) 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

1. INVESTIGATION PROCESS

a) Establish and confirm:

(i) Dates of breach and report

(ii) Responsive actions taken so far

(iii) Nature of the breach: unauthorized collection, use, disclosure, loss, loss of access, or modification

(iv) Custody and control of the information breached

(v) Extent and scale: distribution, location and volume of information

(vi) Know causes and recipients

(vii) Employees, individuals and organizations involved

b) Investigations establish facts based on evidence collected in documentation, interviews and forensics. Timelines to complete the investigation follow the standards based on level of breach in the Privacy Breach Procedures Table.

2. **FINDINGS**

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

3. **REPORT DISTRIBUTION**

a) If Police are investigating the breach for criminal enforcement purposes, coordinate activities with officers involved.

b) Investigative reports are distributed to Leadership and IT, HR, OIPC and the Police as required. Subject Individuals are given a summary of the findings in accordance with Trochu Collection, Use, Disclosure and Right of Access policies.

STEP 5: REMEDIATION AND PREVENTION

1. **REMEDIATION**

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

2. **PREVENTION RECOMMENDATIONS**

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

3. **DISCIPLINE**

a) Depending on the nature and significance of the breach, the role of employees involved, and the information security policy in place, Trochu can take discipline action against an employee who has violated Trochu policy or applicable legislation. This will be passed to Leadership for resolution.