	Town of Cochrane Policy
Policy Title:	**Privacy, Access and Security Policy**
Approval Date:	**June 8, 2026**
Department:	**Legislative Services**

Policy Statement

The Town of Cochrane is committed to providing full informational accountability and to protecting the privacy of individual citizens and its employees. To that end, Cochrane has implemented a privacy and access program to meet the following goals and principles.

1. REASON FOR POLICY

The *Alberta Access to Information Act* ("ATIA") ensures individual right of access to information and protects the personal information of the public, and employees of public bodies operating in Alberta. The Town of Cochrane ("Cochrane") is bound by the requirements of the *Protection of Privacy Act* ("POPA") and collects, uses, and discloses personal information in accordance with its provisions. This policy establishes the principles and processes for managing Cochrane information in compliance with ATIA and POPA.

1.1. Scope

This policy applies to:

1.1.1. All individuals performing services for Cochrane, including all permanent and temporary employees, elected and appointed officials, students, volunteers, and all persons under a contract or agency relationship.

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

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

1.2. Goals and Principles

Cochrane is committed to providing full informational accountability and to protecting the privacy of individual citizens and its employees. To that end, Cochrane has implemented a privacy and access program to meet the following goals and principles:

1.2.1. PROGRAM ACCOUNTABILITY

Cochrane designates a position and individual who is accountable for implementing and maintaining access to information and privacy for information under the custody or control of Cochrane.

1.2.2. OPENNESS

Cochrane develops and follows access, privacy and security policies and practices that are compliant with legislation. Such policies and practices are publicly available.

1.2.3. COLLECTION OF PERSONAL INFORMATION

Cochrane collects personal information only for authorized purposes and collects the least amount of personal information with the highest degree of anonymity required for the authorized purpose.

1.2.4. IDENTIFYING PURPOSES

When collecting personal information directly from an individual, the individual is informed of the purpose for which the information is collected.

1.2.5. LIMITED USE, AND DISCLOSURE OF PERSONAL INFORMATION

Personal information is only used and disclosed in accordance with the purpose for which it was collected, unless alternate use or disclosure is authorized or required by law, or with the knowledge and consent of the subject individual.

1.2.6. ACCURACY

Cochrane makes all reasonable efforts to ensure that both general information and personal information created or received by Cochrane is accurate and complete. Individuals who believe there is an error or omission in their personal information have a right to request correction or amendment of the information.

1.2.7. RIGHT OF ACCESS

Individuals have a right of access to all information, including personal information about themselves, that is in Cochrane's custody or control, subject to limited and specific exceptions.

1.2.8. SAFEGUARDS

Cochrane protects personal information in its custody or control by deploying security measures and practices to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, or destruction.

1.2.9. COMPLIANCE CHALLENGES

Individuals are encouraged to bring any concerns or issues regarding privacy and access at Cochrane to the Privacy and Access Officer for discussion and response. The Privacy and Access Officer will investigate and respond to the individual. Individuals may appeal to the Information and Privacy Commissioner of Alberta to review or investigate Cochrane right of access or correction responses, or any policies or practices that they feel are not in compliance with legislative requirements.

1.3. Quality Controls and Assurance

1.3.1. POLICY REVIEW AND ASSESSMENT

Cochrane reviews and assesses Privacy, Access and Security policies annually to ensure that they are effective and align with legislative, regulatory or Cochrane functional developments and changes.

1.3.2. TRAINING AND COMMUNICATION

a) All Cochrane employees are provided with regular training resources to ensure they adequately understand and can implement all aspects of the Privacy, Access and Security program. Training is ongoing and refreshed or expanded upon in regular intervals in accordance with the roles and responsibilities of employees.

b) Training resources are reviewed annually to ensure that they are effective and align with legislative, regulatory or Cochrane functional developments and changes.

1.3.3. PRIVACY, ACCESS, AND SECURITY MONITORING AND ASSESSMENT

a) Systems, circumstances, practices or repositories that pose a potential risk or gap in standards relating to the privacy, accessibility, usability, integrity, retention, continuity, and security of Cochrane information are identified, monitored and assessed to determine the extent of the risk and the mitigation required.

b) Cochrane will identify all systems collecting personal information and will establish requirements for audit logging, monitoring and review of electronic systems that collect, use, disclose or store personal information, data derived from personal information and non-personal data.

1.3.4. PERSONAL INFORMATION INVENTORY, PERSONAL INFORMATION DIRECTORY, AND PERSONAL INFORMATION BANKS

a) Cochrane is committed to the responsible management, protection and transparency of personal information in its custody or under its control. In support of this commitment Cochrane supports the development and maintenance of a personal information inventory.

b) A personal information inventory is a comprehensive list of all personal information held by Cochrane. It includes data storage locations, categories of personal information categories of individual whose personal information it holds, the purposes for collection, use and disclosure and the sensitivity and security classification of this personal information. The personal information inventory may be incorporated in records management systems and processes.

c) Cochrane creates and maintains a directory of the personal information banks under its custody and control.

d) Cochrane publishes the directory of its personal information banks, either in printed or electronic form, and makes it available to the public.

e) The personal information bank directory includes:

(i) the title of the personal information bank;

(ii) the location of the personal information bank;

(iii) a description of the types of personal information;

(iv) a description of the categories of individuals whose personal information is included;

(v) the authority for collecting the personal information;

(vi) the purposes for which the personal information was collected or compiled; and,

(vii) the purposes for which the personal information may be used or disclosed.

f) If personal information is used or disclosed for a purpose other than the one described in the directory, Cochrane

(i) keeps a record of the purpose and connects that record to the personal information; and,

(ii) updates the directory to include the new purpose in the next publication of the directory.

1.3.5. PRIVACY IMPACT ASSESSMENTS

a) Privacy Impact Assessments (PIAs) are completed for any systems, programs, services, projects or practices that introduce significant new or expanded collection, use, disclosure, processing or security exposure of personal information.

b) The introduction of, or change to, a system, program, service, project or practice is considered significant if:

(i) the loss of, unauthorized access to or unauthorized disclosure of the personal information involved could result in significant harm;

(ii) it involves highly sensitive information;

(iii) it involves personal information of a significant percentage of the Cochrane's service population;

(iv) there is data matching of personal information with an external electronic information repository;

(v) it is part of a common or integrated service or program;

(vi) the technology used is innovative; or

(vii) the administrative, technical, or physical measures and systems being proposed represent an additional risk to the privacy of individuals.

c) Any projects or changes of such nature are reported to the Privacy and Access Officer or designate, who is responsible for completing the PIA in conjunction with the project manager.

d) PIA content standards follow requirements set by the Office of the Privacy Commissioner of Alberta. The PIA is completed and submitted to the Office of the Privacy Commissioner of Alberta before the project is implemented where possible.

1.4. Terms and Definitions

1.4.1. "AI Inference" is the process by which a trained AI model takes input data and produces an output, based on conclusions and reasoning.

1.4.2. "Artificial Intelligence Service (AI Service)" are computer programs and applications that complete tasks and generate information that normally requires human intelligence such as evaluation, problem-solving, reasoning, and decision-making, using machine-based learning. Also considered an automated system.

1.4.3. "Authorized Representative" is any person who can exercise the rights or powers of an individual. This includes the right of access to an individual's personal information and the power to provide consent for disclosure of such information. This may include:

a) an executor or administrator of the estate of an individual who is deceased, for purposes of administering the estate
b) a guardian or trustee of a dependent adult, according to appointment under law
c) an agent under a personal directive, in accordance with the directive
d) an individual who is acting under specific provisions of a power of attorney
e) a guardian of a minor under 18 years of age, excluding mature minors, if the exercise of the rights or powers of the guardian would not be an unreasonable invasion of the personal privacy of the minor
f) an individual acting with the written authorization of an individual

1.4.4. "Collection" means to gather, acquire or obtain personal information about an individual, from any source, including third parties.

1.4.5. "Common or Integrated Service or Program" is a program or service planned, administered, delivered, managed, monitored or evaluated by Cochrane working collaboratively with one or more other public bodies or another public body working on behalf of Cochrane or Cochrane and one or more other public bodies.

1.4.6. "Confidentiality" means a condition or status in which collection, use, or disclosure of information is restricted to specific persons for specific purposes. When and how the collection, use and disclosure restrictions are

applied and maintained are defined by legislation and policy.

1.4.7. "Consent" an informed agreement by an individual to the use or disclosure of their own personal information held by a public body, which can be revoked by the individual at any time.

1.4.8. "Custody or Control" custody is the effective physical possession of information; control is responsibility and accountability for making decisions about the handling of information, regardless of whether Cochrane has custody of the information. Cochrane has control over any information that any of its officials, employees, or service providers has created or received as part of their mandated functions and activities, regardless of the location of the information or the time of collection, use, or disclosure.

1.4.9. "Data Derived from Personal Information" means data created or is obtained from data matching that identifies individuals whose personal information was used in the data matching process. May include AI Inferences.

1.4.10. "Data Matching" is the linking of personal information between 2 or more databases or other electronic sources of information.

1.4.11. "Disclosure" means giving access to or making the personal information in Cochrane's custody or control available to a person or organization external to Cochrane.

1.4.12. "Employee" is all individuals performing services for Cochrane, including all permanent and temporary employees, elected and appointed officials, students, volunteers, and all persons under a contract or agency relationship

1.4.13. "External Networked Source" interconnected computer networks, such as the internet, that contain information for which Cochrane has little to no control over content creation, integrity or disclosure.

1.4.14. "High Sensitivity Information" means personal information about an individual that is:

a) biometric information;
b) financial information; or
c) personal information about a minor, senior or vulnerable person.

1.4.15. "Individual" any person, living or deceased, regardless of residency, citizenship, or status. In addition, the authorized representative of the individual.

1.4.16. "Large Language Model (LLM)" is the language model of an AI Service that has been trained using vast amounts of data to learn patterns and

language that generate human-like inferences.

1.4.17. "Law Enforcement" means policing, including criminal intelligence operations, security or administrative investigation that leads or could lead to a penalty or sanction.

1.4.18. "Mature Minor" means an individual under the age of 18 who has the capacity to make their own decisions about significant matters affecting them, demonstrated by their independence, psychological stability, intellectual capacity, and/or life situation. In the case of privacy, the guardian of a mature minor would not be considered their authorized representative.

1.4.19. "Notification" is an explanation of policies, procedures, consequences, and risks related to the collection, use or disclosure of an individual's personal or personal employee information. Cochrane must properly inform and notify individuals and employees that personal information is being collected, the purposes for which it is being collected, and who may be contacted at Cochrane if an individual has questions about the management of their personal information.

1.4.20. "Non-personal Data" is data, including data derived from personal information and synthetic data, that has been generated modified or anonymized so that it does not identify any individual.

1.4.21. "Personal Employee Information" is personal information collected, used, or disclosed solely for the purposes of establishing, managing, or terminating an employment or volunteer relationship.

1.4.22. "Personal Information" is information about an identifiable individual including:

a) name;
b) address, telephone, email, or contact information*;
c) race;
d) national or ethnic origin;
e) colour;
f) religion;
g) political beliefs or associations;
h) age;
i) sex;
j) marital status;
k) family status;
l) identifying numbers;
m) fingerprints or blood type;
n) educational, financial, employment, criminal records;
o) opinions about the individual; and
p) individual's personal views or opinions (except opinions about others).

**Business address, telephone, email or other contact information of an employee of a public body, or any individual is not personal information, if it is provided on behalf of the employer in the individual's capacity as employee or agent.*

Personal information under ATIA and POPA that is not normally excepted from disclosure:

q) opinions contained in work product
r) classification, salary range, discretionary benefits, or employment responsibilities of public body employees
s) financial and other details of a contract to supply goods or services to a public body
t) information about a license, permit, financial or other discretionary benefit granted to an individual by a public body
u) information is about an individual who has been dead for 25 years or more
v) information is about an individual's enrolment at a school, attendance at a public event, or receipt of an award granted by a public body

1.4.23. "Personal Information Bank (PIB)" is an information repository that is organized or retrievable by an individual's name or other identifier.

1.4.24. "Privacy Impact Assessment (PIA)" is a review and explanation of proposed changes in practices, programs or information systems affecting the collection, use, disclosure, or security of personal information under the custody or control of a public body. At the early stages, the PIA will identify practices and risks that should be addressed, amended, or mitigated before implementation of the program or system.

1.4.25. "Prompt" is a queue, instruction, or question given to an AI Service to elicit a response, action, or creative output.

1.4.26. "Reasonable Security Arrangements" are administrative, physical and technical safeguards to protect personal information, data derived from personal information and non-personal data in the custody or under the control of Cochrane that are appropriate and proportional with the security classification level of the information and in the case of non-personal data, ensure to the extent possible, that the identity of the an individual who is the subject of non-personal data cannot be re-identified from the data.

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

1.4.28. "Research" means academic, applied, or scientific research, excluding internal program or quality improvement assessments, that necessitates the use of individually identifying personal information.

1.4.29. "Severing" means in a right of access request, separating or hiding/redacting information in a document that should or cannot be released so that the remainder of the document can be disclosed.

1.4.30. "Significant Harm" is harm that results from the unauthorized access, disclosure, or loss of personal information, including:

a) bodily harm;
b) humiliation;
c) damage to reputation or relationships;
d) loss of employment or business or professional opportunities;
e) identify theft;
f) diminished insurability;
g) diminished credit;
h) loss of property or legal status; or
i) loss of finances.

The following factors are also considered in determining the significance of harm:

j) it is reasonably believed that the information has been or will be misused;
k) the unauthorized access, disclosure of loss was the result of malicious intent;
l) the personal information is sensitive; or
existing mitigating factors reduce the risk of significant harm.

1.4.31. "Third Party" is a person, a group of persons or an organization other than the applicant making an access request, or other than the employees and officials of Cochrane.

1.4.32. "Use" means use of information by Cochrane employees for an authorized purpose that is authorized by policy or law.

1.5. Roles and Responsibilities

1.5.1. HEAD

a) Unless otherwise delegated, the Head of Cochrane is responsible for all obligations and discretionary decision-making under ATIA and POPA.
b) The Head of Cochrane has been delegated to the Director, Legislative & Administrative Services.
c) The Head has delegated powers, duties and obligations under ATIA and POPA to the Privacy and Access Officer in accordance with the functions and activities set out in section 1.5.2.

d) The Head has delegated powers, duties and obligations under ATIA and POPA to the Privacy and Access Coordinator in accordance with the functions and activities set out in section 1.5.3.

1.5.2. PRIVACY AND ACCESS OFFICER (PAO)

The PAO is delegated by the Head to be responsible for the overall management and coordination of privacy, security and access to information at Cochrane in accordance with the delegation order. The PAO is responsible for the following functions and activities:

Program Management

a) Ensuring that privacy, access and security program policies and procedures are developed, maintained, and updated, compliant with legislation.
b) Ensuring that developing and completing quality assurance processes for implementation of Cochrane organization privacy and access management.
c) Ensuring that training and resources are provided so that Cochrane employees, volunteers and contracted personnel are fully knowledgeable of their privacy and access duties, roles, responsibilities and practices in compliance with policy and legislation.
d) Representing Cochrane in dealings with third parties, the provincial government, and the Office of the Privacy Commissioner of Alberta, as necessary.
e) Directing the response to privacy breaches of personal information at Cochrane and its facilities in line with legislation and the Privacy Breach Response Policy.

1.5.3. PRIVACY AND ACCESS COORDINATOR (PAC)

The Privacy and Access Coordinator is delegated to be responsible for the overall function of privacy, security and access to information at Cochrane in accordance with the delegation order. The Privacy and Access Coordinator is responsible for the following functions and activities:

Right of Access, Correction, and Complaints

a) Responding to requests for access to information including, as necessary, assessment of fees, time extensions, disregarding requests, transfer of requests, duty to assist applicants, application of exceptions, third party notifications and public interest disclosure notice.
b) Responding to request for correction of personal information, including, as necessary, transfer of requests, correcting personal information, annotating personal information, notifying recipients.
c) Responding to requests for review of the handling of an access request or a privacy complaint including, as necessary, complaint submission, duty to assist the applicant, communicating with the OIPC, investigation, and responding to the applicant.

d) Providing advice, interpretation and implementation of applicable legislation regarding personal information, including release / non-release, collection, use and disclosure of personal information.
e) Ensuring the security, protection and accuracy of personal information in the custody or control of Cochrane in compliance with legislation and policy.
f) Completing Privacy Impact Assessments (PIAs) for Cochrane in conjunction with project managers for project-specific personal information systems and practices.
g) Developing and maintaining a directory of Personal Information Banks and other registries required for identifying and tracking the collection, use, disclosure and security of personal information.

1.5.4. SENIOR MANAGEMENT AND TOWN COUNCIL

a) Senior Management and Town Council are responsible for ensuring that privacy, access and security policy and practices in Cochrane are aligned with governing mandates, standards, and planning.

1.5.5. INFORMATION TECHNOLOGY (IT) MANAGEMENT

IT Management, in coordination with the PAO, is responsible for all systems, networks and applications, as follows:

a) implements and deploys privacy and security measures;
b) completes risk and mitigation assessments;
c) monitors and detects security threats;
d) assists in the response to privacy breaches.

1.5.6. MANAGEMENT

Department Managers are responsible for implementing privacy and security policies and practices within their functional areas and are accountable for adherence to all policies by their employees and contracted third parties.

Management:

a) supports their employee’s awareness of and training on privacy and security policies and procedures;
b) implements privacy and security standards and processes in compliance with policy as they relate to information repositories and operational functions and activities of their area;
c) provides appropriate resources and facilities as needed to support the implementation of privacy and security policy in the department;
d) refers all formal right of access requests for information to the Privacy and Access Coordinator;
e) cooperates and assists in locating and retrieving departmental information relevant to right of access requests;

f) reports gaps in privacy, access and security policy affecting their areas to the Privacy and Access Coordinator;
g) reports any new information repositories or data systems that require registration, assessment, and security classification to the Privacy and Access Coordinator or the Privacy and Access Officer.

1.5.7. ALL COCHRANE EMPLOYEES AND SERVICE PROVIDERS

All Cochrane employees and service providers are responsible for implementing privacy and security for all information they create and receive as part of their functions and activities. Employees:

a) make themselves aware of and adhere to privacy, access and security and standards;
b) at the time of hire or engagement complete an oath of confidentiality;
c) capture, manage, access, release and protect information in their custody or control according to privacy, access and security policy;
d) access, release and protect information in their custody or control according to policy;
e) refer to the Privacy and Access Coordinator for all decisions about collection, use, disclosure, and access that are not clearly directed by policy;
f) report all suspected breaches of personal information to the PAO immediately upon discovery; and
g) identify and report information security incidents to the appropriate manager according to privacy breach procedures (section 6.3).

2. COLLECTION, USE, DISCLOSURE, DATA MATCHING, AND NON-PERSONAL DATA

2.1. Collection of Personal Information

2.1.1. Cochrane collects personal information only if:

a) the collection is expressly authorized by legislation;
b) the information is collected for the purposes of law enforcement; or
c) the information relates directly to and is necessary for an operating program or activity of the public body, including a common or integrated program.

2.1.2. Cochrane collects personal information directly from the individual, or their authorized representative. Cochrane only collects personal information indirectly from another source in the following circumstances:

a) the indirect collection is authorized by the individual, other legislation, or the Alberta Information and Privacy Commissioner;
b) the personal information may be disclosed to Cochrane under the disclosure provisions outlined below;

c) the personal information is collected in a health and safety emergency, and the individual is unable to provide the information;
d) direct collection could reasonably be expected to endanger the mental or physical health or safety of the individual or of any other person;
e) the personal information is about a designated emergency contact;
f) the personal information is required to determine suitability for an honour or award;
g) the personal information is required to verify the individuals' eligibility for participation in a program or to receive a benefit, product, or service from Cochrane;
h) the personal information is collected from public sources for fund-raising;
i) the personal information is required for a law enforcement purpose;
j) the personal information is required to collect a fine or debt owed to the public body, or for use in the provision of legal services to Cochrane;
k) the personal information concerns the history, release, or supervision of an individual under the supervision of a correctional authority;
l) the personal information is required to inform the Public Trustee or Public Guardian about clients or potential clients;
m) the personal information is required for enforcing an order under the Maintenance Enforcement Act;
n) the personal information is required to manage or administer Cochrane personnel;
o) the personal information is required to support researching or validating claims, disputes, or grievances of aboriginal people; or
p) the personal information is required to plan, manage, deliver, monitor and evaluate a common or integrated program or service.

2.1.3. When collecting personal information directly from an individual, Cochrane informs the individual of the purpose for which the information is collected, the legal authority for the collection, any intention to input the information into an AI service and contact information of the individual who can answer questions about the collection.

2.1.4. Notifications are included on the medium or at the location of collection (websites, forms, pamphlets, posters). Notice is not required in circumstances when personal information is collected indirectly, for authorized purposes.

2.1.5. Cochrane employees collect only the amount and types of personal information as required to complete the stated function or purpose.

2.2. Consistent Purposes

2.2.1. ☐Cochrane will primarily use and disclose personal information for the purpose for which it was originally collected or for a consistent purpose.

2.2.2. For a use or disclosure to be for a consistent purpose, Cochrane must determine that the proposed use or disclosure is:

a) directly connected to the original purpose for collection; and

b) necessary for operating a program or common or integrated program or service of Cochrane.

2.2.3. In assessing the consistent purpose, Cochrane must consider:

a) the nature of the original purpose documented at the time of collection;

b) whether the new use or disclosure is a logical extension of that purpose;

c) the expected impact on the individual's privacy.

2.3. Use of Personal Information

2.3.1. Cochrane may use personal information under the following circumstances:

a) for the purposes for which it was originally collected or for a use consistent with that purpose;

b) with the consent of the individual, when obtained in accordance with consent standards; or

c) for a purpose for which the information is disclosed to Cochrane by another public body, under the allowable disclosure provisions.

2.3.2. Cochrane employees use only the amount and types of personal information as required to complete the stated function or purpose.

2.4. Disclosure of Personal Information

2.4.1. Cochrane may disclose personal information for the purpose for which the information was collected or compiled or for a purpose consistent with that purpose;

2.4.2. Cochrane may disclose personal information for an inconsistent purpose only in the following circumstances:

INDIVIDUAL OR PUBLIC INTERESTS

a) with the consent of the individual, when obtained in accordance with consent standards;

b) to avert or minimize a risk of imminent harm and danger to the health and safety of any person;

c) so that the spouse or adult interdependent partner, relative or friend of an injured or deceased individual may be contacted, or to a relative of a deceased individual;

d) personal information of a minor or parent or guardian of a minor, to a law enforcement agency or to another organization or public body providing services to the minor, if it is clearly in the best interest of the minor;

e) to an MLA to assist the individual;

f) if disclosure is not an unreasonable invasion of privacy (Appendix 7.2);

LEGAL OR ENFORCEMENT REQUIREMENTS

g) to comply with, or in accordance with, an enactment of Alberta or Canada;

h) in response to a subpoena, warrant or court order;

i) for law enforcement purposes;

j) for the supervision of an individual by a correctional authority, or to a lawyer or student-at-law acting for an inmate;

k) to comply with the Maintenance Enforcement Act, or to the Administrator of the Motor Vehicle Accident Claims Act;

l) to an Officer of the Legislature if required for their duties;

OPERATIONAL REQUIREMENTS

m) to an officer or employee of Cochrane if necessary for their duties;

n) to an officer or employee of another public body if necessary for planning, managing, delivering, monitoring or evaluating a common or integrated program or service;

o) to enforce a legal right, or to collect a fine or to make a payment, or for court and quasi-judicial proceedings;

p) to verify an individual's suitability or eligibility for a program or benefit;

q) to comply with the public interest disclosure provisions;

r) to the Auditor General or any other prescribed person for audit purposes;

s) to another public body for the authorized purposes of data matching;

HUMAN RESOURCES

t) to a union representative, with the consent of the individual;

u) for the management of personnel;

PUBLIC DISSEMINATION AND RESEARCH

v) to the Provincial Archives of Alberta or to Cochrane archives or another public body archives for archival preservation purposes;

w) for research or statistical purposes, under agreement;

x) when the information is available to the public.

2.4.3. Cochrane employees disclose only the amount and types of personal information as required to perform their assigned duties.

2.4.4. If there is no authority for the disclosure, the information cannot be disclosed. If the individual making the request for information wishes, they may make a formal ATIA Request.

2.4.5. Cochrane will not sell personal information under its custody or control in any circumstance or for any purpose.

2.5. Research Disclosure

2.5.1. Personal information may be disclosed for statistical or research purposes, only if:

a) research cannot reasonably be accomplished in a non-identifiable form or is approved by the Office of the Information and Privacy Commissioner;

b) data matching resulting from the disclosure is not harmful to the individuals the information is about, and the benefits are clearly in the public interest;

c) Cochrane has approved conditions relating to security and confidentiality, removal or destruction of individual identifiers, and prohibition of any subsequent use or disclosure without authorization; and

d) all of the conditions are set out in a written research proposal and agreement

2.6. Data Matching and Non-Personal Data

2.6.1. Cochrane:

a) data matches personal information between two or more information sources to create new data derived from personal information; and

b) creates non-personal data from identifiable personal information;

only for the purposes of:

c) research and analysis; or

d) planning, managing, delivering, monitoring or evaluating a program or service.

2.6.2. For the purposes of data matching, Cochrane:

a) does not collect personal information directly from the individual;

b) may collect personal information from another public body;

c) may use personal information under its custody and control.

2.6.3. Cochrane implements human oversight, auditing and validation measures for systems used for creating data derived from personal information or non-personal data to ensure the accuracy and reliability of the data.

2.6.4. Cochrane retains and uses data derived from personal information only for the purpose for which it was created and as long is reasonably necessary to enable Cochrane to carry out that purpose.

2.6.5. Cochrane discloses data derived from personal information only:

a) to the other public body from which data matched personal information was collected, for the purpose it was created;

b) to the Office of Statistics and information for the purposes of The Office of Statistics and Information Act.

2.6.6. Cochrane uses non-personal data for any purpose and discloses non-personal data to anyone other than another public body only under agreement containing the required conditions, including prohibiting re-identification of individuals.

2.6.7. Cochrane is not restricted from disclosing reports, summaries or other publications containing non-personal data that is aggregate or statistical form.

2.7. Consent Standards

2.7.1. Cochrane can only request the consent of the individual for use or disclosure of their personal information, not for collection.

2.7.2. 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; and

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

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

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

2.7.4. 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.

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

2.8. Research Project Agreements

2.8.1. Researchers are required to submit a Research Proposal for consideration and approval by the PAO.

2.8.2. Cochrane discloses personal information for research purposes only if the recipient signs an agreement.

2.9. Non-Personal Data Best Practices and Requirements

2.9.1. Cochrane develops and implements 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.

2.9.2. When creating non-personal data, and before it is used or disclosed, Cochrane:

a) verifies the effectiveness of methods used;

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

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

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

2.9.3. Cochrane will assess and record the risk and mitigations of risks of its de-identification standards and techniques resulting in re-identification. As part of this assessment Cochrane considers:

a) whether the non-personal data can be matched with other public or internal datasets or sources;

b) whether the number of de-identified individuals in an aggregate or cell associated with specific attributes is too small;

c) whether there are too many other attributes associated with the de-identified individual;

d) whether geolocation data (place and time) are included as attributes associated with the de-identified individual.

2.9.4. Whenever non-personal data is created from personal information under its custody or control, and before it is used, Cochrane records and maintains 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 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.

2.10. Artificial Intelligence

2.10.1. Collection, Use and Disclosure

2.10.1.1. When Cochrane makes use of generative artificial intelligence applications and processes (AI services), personal information is only collected, used, and disclosed in compliance with legislation and policy. The personal information activities may include:

Indirect Collection

a) accessing and compiling personal information from external networked sources or external datasets in response to prompts, either directly or through large language models (LLMs).

b) creation or generation of new personal information as inferences by AI services as a response to user prompts.

Direct Collection

c) collecting information from individuals in conversations or engagements through an AI chatbot service.

Use

d) accessing and compiling personal information from internal sources and datasets in response to prompts, either directly or through LLMs.

e) use of prompts, internal information and datasets, and generated inferences containing personal information to train internal large language models (LLMs).

Disclosure

f) disclosure of prompts and generated inferences containing personal information to external parties.

g) Cochrane considers information about individuals extracted by an AI service from external networked sources, including the internet, as personal information.

h) Cochrane only uses AI services that do not disclose internally generated personal information in prompts or internal information sources to an external LLM for AI training purposes.

i) Cochrane considers inferences generated by an AI service containing personal information as data derived from personal information.

2.10.2. Information Accuracy and Integrity

2.10.2.1. Cochrane does not use or distribute inferences generated by AI services about or affecting individuals before they are reviewed for accuracy and integrity and verified by competent and qualified employees.

2.10.2.2. Inferences generated by AI services for Cochrane use include citations and references to sources detailed enough to verify the veracity and completeness of the information.

2.10.3. Notification

2.10.3.1. Cochrane notifies individuals that AI Services have and are being used to:

a) collect personal information in conversations or direct engagements with individuals; or

b) generate information or knowledge that contributes to decision-making about the individual.

2.10.3.2. Notifications contain all the elements of a collection notice with the addition of a statement that information or knowledge from AI services has contributed to decision-making about the individual.

2.10.3.3. Upon request, Cochrane provides:

a) the name and description of the AI services used; and

b) citations of the sources used by the AI Services to generate inferences that contributed to decision-making about the individual.

2.10.3.4. This notification may not be provided in cases where one of the circumstances or conditions which require or allow Cochrane to withhold the information apply.

2.10.4. Regulation of Use

2.10.4.1. Cochrane controls and regulates the use of AI for specified purposes based on the risk to individuals.

2.10.4.2. Cochrane considers the following activities using AI services as high-risk:

a) health assessment and diagnosis;

b) human resource performance evaluation and recruitment;

c) safety components and controls for critical equipment and infrastructure;

d) assessment of individuals requesting access to essential human services;

e) predictive profiling;

f) biometrics-based recognition and identification, including images.

2.10.4.3. Cochrane employees complete high-risk AI activities only with the approval of the Privacy and Access Head, who evaluates the risk on a case-by-case basis.

2.10.4.4. All new high-risk AI activities require a Privacy Impact Assessment, which may require an Algorithmic Impact Assessment, before they are initiated.

2.10.4.5. Cochrane considers the following activities using AI services as low risk:

a) content generation and editing;

b) computer and program coding;

c) information indexing and search;

d) spam and malware filtering;

e) audit logging and monitoring;

f) recommendations for routine or transactional activities.

2.10.4.6. Cochrane employees complete low-risk AI activities as required for their role based on their effectiveness for the purpose.

2.10.4.7. Where practical and effective for purpose, Cochrane implements mitigating conditions and activities that mitigate the risks associated with AI services, such as:

a) limiting an AI service to a small-scale information system and LLM model to support a narrowly defined purpose or function;

b) completing pre-implementation testing and monitoring of AI services performance for the identified purpose;

c) implementing human oversight to ensure the accuracy and reliability of the AI services;

d) continuously monitoring the effectiveness of AI services for the activity.

3. RIGHT OF ACCESS AND CORRECTION OF INFORMATION

Subject to limited and specific exceptions, individuals have a right of access to information that is in the custody or control of Cochrane. Further, individuals have a right to request correction or amendment of information about themselves. This policy is intended to define a process for facilitating requests for access to personal information, or to correct or amend personal information.

3.1. Receiving and Facilitating Requests

3.1.1. Requests for access to Cochrane information can be made by any individual or organization (the applicant), regardless of location or status. A public body may not make a request to another public body.

3.1.2. Cochrane responds to right of access requests openly, accurately and completely and will:

a) engage with applicants to allow them to clarify their request so it can be processed

b) respond to questions in plain language, and,

c) assist applicants in adjusting requests so they can be processed.

3.1.3. Cochrane does not deny access to information based on the applicant's reason or purpose for the request.

3.1.4. Requests for information under ATIA may contain personal information of the applicant, which will be protected and managed in accordance with POPA.

3.1.5. Once the applicant has met the requirements to make a request, Cochrane has 30 business days to respond, unless the request has been abandoned, disregarded or transferred, or if the time limit is extended in accordance with ATIA.

3.2. Excluded Records

3.2.1. Some records that are in the custody or control of Cochrane are excluded from the ATIA and do not have to be considered relevant or released as part of a right of access request. However, Cochrane may choose to release this

information as part of a request under specified circumstances. Excluded records include:

a) records designated by Cochrane as available without a request;

b) court and administrative support records created or received by the courts of Alberta, including justices of the peace;

c) records created or received by officers of the Alberta Legislature, including the Office of the Information and Privacy Commissioner, Ethics Commissioner, Auditor General, and the Public Interest Commissioner;

d) records and copies of records from a provincial or public body registry office, including the Personal Property Registry, Corporate Registry, Motor Vehicles Registry, Land Titles Office, and the Vital Statistics Registry;

e) Cochrane records that have already been made public by other means;

f) records in the custody or control of the federal, provincial or territorial government and their agencies;

g) personal or constituency records of an elected or appointed member of the governing body of Cochrane;

h) health records created or received by a Cochrane doctor or nurse;

i) a question used on an examination or test only if release does not jeopardize a standardized or continuing evaluative process.

3.2.2. These excluded records can only be used or disclosed with the consent or permission of the individual or organization:

a) Records from private sector donors that are preserved in Cochrane archives for historical research purposes.

3.2.3. Data derived from personal information and non-personal data cannot be released in response to a right of access request.

3.3. Disregarding Requests

3.3.1. Cochrane disregards a right of access request only in exceptional circumstances when:

a) the information requested is already available to the applicant or to the public;

b) after initial requests from Cochrane for clarification, the applicant has not provided enough detail to make it comprehensible or to locate the requested information;

c) the request has been made repeatedly, as part of a pattern of conduct that is systematic, regular and deliberate;

d) the applicant makes use of abusive, threatening, or harassing language or actions during the application or facilitation process; or

e) the request is abusive, threatening, frivolous or vexatious.

3.3.2. The applicant is informed of the reasons for disregarding the request and the right to ask the Commissioner to review Cochrane's decision.

3.4. Searches for Relevant Records

3.4.1. Cochrane makes every effort to identify and retrieve for review all records in its custody or control that are relevant to an applicant's request. This will include information in any location and format and on any devices, accounts and platforms not owned by Cochrane, that was created or received by employees and contractors to support their functions as Cochrane officials.

3.4.2. The search for records relevant to an applicant's request includes all electronic records that can be accessed or produced using normal computer hardware, software and technical expertise and would not unreasonably interfere with its operations. This includes:

a) reports or extracted data sets from existing databases that can be constructed and generated using existing software and expertise, but does not include the creation of information that is an analog summary, analysis, consolidation or digest of existing information that did not exist prior to the request;

b) emails, text messages, and social media posts sent or received on any account or platform that were created or received to support functions and activities of Cochrane.

3.4.3. Cochrane Privacy and Access officials responsible for responding to a request are authorized to access and retrieve for review any personal or general information on any device or platform that is required to identify, retrieve records relevant to a request.

3.5. Reviewing and Withholding Information

3.5.1. Cochrane only withholds information relevant to the request when it is determined that mandatory or discretionary or exceptions to the right of access apply to the records requested.

3.5.2. Cochrane must refuse to disclose information in response to a right of access request if the release would be:

a) harmful to business interests of a third-party business;

b) an unreasonable invasion of a third party's personal privacy; or

c) harmful to provincial Cabinet and Treasury Board confidences, as long as the information is in a record for less than 15 years or result in the release of a record that was submitted to or prepared for submission to the Executive Council, the Treasury Board or one of their committees, or was created on or on behalf of any of the above.

3.5.3. Cochrane may refuse to disclose information in response to a right of access request if the disclosure could reasonably be expected to:

a) threaten anyone's safety or mental or physical health; interfere with public safety; or cause an applicant to do immediate and grave harm to themselves or others;

b) reveal confidential evaluations conducted pre-hire or pre-contract award;

c) harm a law enforcement matter;

d) harm a workplace investigation;

e) harm inter-governmental relations;

f) reveal local public body confidences, including drafts of bylaws, resolutions, legal instruments and the substance of deliberations of in-camera meetings;

g) reveal advice, proposals, recommendation, analyses or policy options developed by or for the public body;

h) cause harm to the economic interests of Cochrane or the Alberta Government;

i) reveal information relating to testing or auditing procedures;

j) reveal legally privileged information;

k) cause harm to conservation of heritage sites; or

l) reveal information that is already or will be made available to the public within 60 business days.

3.6. Public Health and Safety Override

3.6.1. Cochrane discloses without delay, to the public, a group of people, an individual, or an applicant, any information that Cochrane has about a risk of significant harm to the environment or to the health and safety of the public, a group of people, an individual or an applicant.

3.6.2. Before disclosing the information, Cochrane must, where practicable, notify any third party to whom the information relates, give the third party an opportunity to make representations relating to the disclosure and notify the Commissioner.

3.7. Third Party Reviews

3.7.1. Cochrane notifies and requests advice from affected third parties when it is unclear whether the relevant records hold information that, if released, would be:

a) harmful to business interests of a third-party business;

b) an unreasonable invasion of a third party's personal privacy.

3.8. Requests for Correction or Amendment of Personal Information

3.8.1. Individuals may request correction or amendment of their own personal information in the custody or control of Cochrane.

3.8.2. Cochrane will not amend professional opinions that are made by employees that have the competency to make them.

3.9. Right of Access Intake

3.9.1. 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.

3.9.2. Requests for access to information from an individual applicant that may involve review and severing must be in writing to the Privacy and Access Coordinator. 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.

3.9.3. 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.

3.9.4. 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.

3.9.5. 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.

3.9.6. 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.

3.9.7. Within 15 business days after Cochrane 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. Cochrane Privacy and Access Coordinator will notify the applicant of the transfer.

3.10. Fees

3.10.1. 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 7.1).

3.10.2. 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.

3.10.3. A $25.00 administration fee is charged for requests for general information and is non-refundable. A $50.00 administration fee is charged for continuing general information requests. Additional fees may be charged for

reformatting, reproduction, disclosure preparation or transmission of information for general requests, only when the estimated costs exceed $150.00.

3.10.4. 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.

3.10.5. If the applicant requests a waiver of fees, 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.

3.10.6. 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.

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

3.11. Retrieval And Review of Relevant Records

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

3.11.2. 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.

3.11.3. 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. The reviewer may consult with appropriate employees to determine the application of severing.

3.12. Third Party Reviews

3.12.1. If the Privacy and Access Coordinator decided 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.

3.12.2. 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;

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

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

3.12.4. 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.

3.12.5. 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.

3.12.6. 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.

3.13.Response To Applicant

3.13.1. 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.

3.13.2. 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.

3.13.3. Requested information will be provided in a form that is generally understandable. Cochrane 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.

3.13.4. 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.

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

3.14.Time Limits for Responding to a Request

3.14.1. Cochrane responds to right of access requests within 30 business days of the receipt of the request.

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

3.14.3. 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;

3.14.4. 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.

3.14.5. The timelines are automatically extended in:

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

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.

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

3.15. Correction or Amendment Request Processes

3.15.1. 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.

3.15.2. Cochrane 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.

3.15.3. Formal requests to correct or amend information subject to review must be in writing to the 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.

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

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

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

3.15.7. Cochrane 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 Cochrane’s decision.

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

3.15.9. 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 ongoing provision of services.

3.16. Individual Challenges to Request Responses

3.16.1. Individuals are encouraged to bring any concerns or issues concerning responses to requests and compliance with this policy initially to the Privacy and Access Officer for discussion and mediation. Formal complaints regarding a request will be handled in accordance with the Complaint Resolution policy. 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.

4. COMPLAINT RESOLUTION

4.1. Submission

4.1.1. Members of the public may submit a complaint in writing to Cochrane for investigation and resolution. Verbal complaints will not be treated as formal complaint submissions by Cochrane.

4.1.2. Complaints may concern any decision, act, or failure to act by Cochrane in a formal access to information request or in the protection of personal information, data derived from personal information, and non-personal data under Cochrane's custody or control or by a Cochrane employee, including:

a) a contravention in the creation, collection, use, or disclosure of personal information, data derived from personal information, or non-personal data;

b) a refusal, without justification, to a correction of personal information;

c) the actual or attempted re-identification, by any person, of non-personal data;

d) failure by a Cochrane employee to provide a duty to assist;

e) a contravention in the application of a time extension in a formal access request;

f) the inappropriate levy of a fee applied in a formal access request.

4.1.3. Complaints related to unauthorized disclosure, use, destruction, loss, removal or modification of personal information will initiate the privacy breach response process, which may proceed in conjunction with the complaint process.

4.2. Principles of Investigation and Response

4.2.1. The Privacy and Access Officer receives, processes, investigates, and responds to complaints under ATIA and POPA made to Cochrane.

4.2.2. If an investigation is required to establish findings for a complaint, Cochrane uses generally accepted investigative methods to obtain the most effective results while respecting the rights, privacy, and dignity of the complainant and any employees involved. Complaint investigations will, as required, incorporate the following methodologies:

a) keep investigation information confidential to protect the privacy of the complainant and any individuals investigated and to maintain the integrity of the investigation;

b) use surveillance or monitoring data to establish past or current actions on an as-needed basis;

c) examine or confirm the veracity of facts or statements, sometimes using third party witnesses;

d) base findings and conclusions on balance of probabilities.

4.2.3. Records created, collected, or processed as part of a complaint investigation are classified according to the Information Security Classification system and will not be provided as part of the complaint response. Requests by the complainant for investigation records associated to the complaint will be treated as a formal access to information request, and records will be handled according to that process.

4.2.4. The complaint investigation is an administrative rather than a disciplinary process. Once the findings are determined, it is the responsibility of Management and Human Resources to determine the appropriate disciplinary action for employees involved, if any.

4.3. Response

4.3.1. Cochrane acknowledges, in writing, receipt of the complaint. All acknowledgements of submission will include:

a) reference to the initial complaint;

b) an internal assigned file number; and

c) the estimated date of response, within 30 business days of the date the complaint was received.

4.3.2. Cochrane provides responses in writing, containing the findings of the Privacy and Access Head, to all formal complaint submissions.

4.3.3. Response time is dependent on the need for an investigation and the complexity of the associated investigation.

4.3.4. The complaint response will include the following:

a) the internal assigned file number;

b) a copy of the original complaint submission and a list of any records the complainant submitted with the complaint;

c) the findings of the Privacy and Access Head and the reason for the findings or a statement of justification; and

d) contact information for the Office of the Information and Privacy Commissioner and directions for submitting a request for review to the Commissioner.

4.4. Receiving Submissions

4.4.1. The Privacy and Access Officer reviews the submitted complaint to establish if it is submitted under ATIA or POPA and assign an internal file number:

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.

4.4.2. If the scope or nature of the complaint is unclear, the Privacy and Access Officer will contact the complainant to clarify it.

4.5. Acknowledge Receipt of Submission

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

4.6. Investigation And Analysis

4.6.1. The Privacy and Access Officer determines the scope and nature of the complaint according to the parameters established in section C.1.1.3. and records the investigation scope as part of the complaint investigation file.

4.6.2. Based on the context of the complaint, the Privacy and Access Officer 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.

4.6.3. The Privacy and Access Officer will review the complaint with the Privacy and Access Head and with any employees associated with it. If more than one employee is associated with the complaint, the Privacy and Access Head 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.

4.6.4. The Privacy and Access Head 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.

4.6.5. 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.

4.7. Final Response

4.7.1. When the findings of the investigation are determined, a final written response will be provided to the complainant according to the parameters set out in section 4.3.

4.7.2. 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.

4.8. Resolution

4.8.1. 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 Officer may identify further administrative, technical and physical safeguards that can be implemented to modify or prevent future contraventions in Cochrane systems, processes, and employee behaviours. This may include employee or user training, introduction of additional security technology, or upgrade to facilities or infrastructure.

5. INFORMATION SECURITY

The information security provisions of POPA require Cochrane 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. This policy outlines administrative, technical and physical safeguards in place at Cochrane to protect confidential information.

5.1. Safeguards

5.1.1. ADMINISTRATIVE

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

5.1.1.2. The need for confidentiality and security of personal information is addressed as part of the conditions of employment for Cochrane 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.

5.1.1.3. All individuals performing services for Cochrane, including all permanent and temporary employees, elected and appointed officials, students, volunteers, and all persons under a contract or agency relationship on behalf of Cochrane; that collect, use, disclose or have access to

confidential information as part of the performance of their duties for Cochrane, will sign a Confidentiality Agreement.

5.1.1.4. 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.

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

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

5.1.1.7. Cochrane employees and persons acting on behalf of Cochrane report all violations and breaches of information security as soon as possible to Cochrane'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.

5.1.1.8. 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 bylaws and schedules of Cochrane.

5.1.2. PHYSICAL

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

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

5.1.2.3. Cochrane'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.

5.1.2.4. 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.

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

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

5.1.2.7. 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.

5.1.2.8. 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 Cochrane has ended.

5.1.2.9. 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.

5.1.2.10. 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.

5.1.2.11. Cochrane employees will verify the identity and credentials of courier services used for the transportation of personal information.

5.1.2.12. Fax machines and printers that may be used to send or receive confidential information are located in a secure area. Employees use the "safe print" feature and send encrypted faxes when possible. Whenever possible employees will use preprogrammed numbers to send fax transmissions and will review the numbers every 6 months to ensure they are still accurate. 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.

5.1.2.13. Information that is not confidential or sensitive in nature will be destroyed. Confidential or sensitive information is destroyed by shredding. Destruction of records subject to Cochrane's retention and destruction schedule will be documented by listing the records and / or files to be destroyed, the date of destruction, and an employee's signature to confirm that the destruction occurred. The destruction of transitory records does not need to be documented.

5.1.2.14. 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.

5.1.3. TECHNICAL

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

5.1.3.2. Access to data and application systems to personal information is limited by each Cochrane 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.

5.1.3.3. Employees of Cochrane 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.

5.1.3.4. Access to Cochrane information systems is controlled and password protected. Passwords are kept confidential at all times, and are not written down, posted publicly, or shared with other employees. 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 logout requiring authentication to re-enter the system.

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

5.1.3.6. 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. E-mail messages must also contain a confidentiality notification).

5.1.3.7. 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.

5.1.3.8. Cochrane do not use service providers, including cloud services, that require the storage of personal information outside of Canada.

5.1.3.9. Computer systems that hold critical or sensitive information will be backed up on a daily 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.

5.1.3.10. Cochrane monitors AI services and applications to ensure that there is no leakage of internal inferences and other information to external parties.

5.2. Information Security Classifications

5.2.1. CLASSIFICATION LEVELS AND ASSIGNMENT

5.2.1.1. Information will be classified according to the degree of harm that may result from unauthorized access, loss, or modification. Classified as:

a) Restricted

b) Confidential

c) Internal

d) Public

5.2.1.2. Employees will 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.

5.2.2. SECURITY ZONES

5.2.2.1. Physical spaces and logical areas within electronic systems and networks are identified as having the status of one of four security zones, based on the functionality of the area:

a) RESTRICTED: Used infrequently by a subset of authorized individuals with special status for storing and accessing information on a limited basis.

b) INTERNAL: Used regularly by authorized individuals working within the zone for storing and accessing information among them.

c) EXTERNAL: Used regularly by a controlled number of unauthorized and authorized individuals for storing, accessing, and transmitting information among them within the zone.

d) PUBLIC: Used regularly by both authorized and unauthorized individuals for other, uncontrolled purposes.

5.2.2.2. Cochrane will maintain standards to ensure the integrity of each zone, including definition of perimeters, barriers to access, and security practices and equipment within the zone. Physical Security Zones Requirements Table and the Network Security Zones Requirements Table provide details of standards required for each zone.

5.3. Audit Logging

5.3.1. LOGGING REQUIREMENTS

5.3.1.1. Cochrane ensures that all systems containing personal information, data derived from personal information and non-personal data:

a) Generate audit logs that record:

(i) user access (successful and failed attempts)

(ii) creation, modification and deletion of records

(iii) data exports, downloads or transmissions

(iv) changes to user permissions or roles

(v) administrative and privileged activities

b) Capture sufficient detail, including:

(i) user ID

(ii) date and time

(iii) type of activity performed

(iv) system or data accessed

5.3.2. MONITORING AND REVIEW

5.3.2.1. Audit logs are actively monitored to detect:

a) unauthorized access or anomalous behavior

b) bulk access or extraction of information

c) data integrity issues

d) repeated failed login attempts

5.3.2.2. Formal log reviews occur on a scheduled basis, relative to the information security classification of the information contained within the system and following any suspected or confirmed privacy breach.

5.3.3. LOG RETENTION AND SECURITY

5.3.3.1. Audit logs are retained in accordance with applicable Cochrane retention schedules, with a minimum retention period of at least 12 months.

5.3.3.2. Audit logs are protected from unauthorized access, alteration or deletion by:

a) restricting access to authorized employees only

b) storing logs securely and encrypting where appropriate

c) implementing mechanism to detect log alteration

5.3.3.3. Individuals with administrative access are not the sole reviewers of logs where practical and reasonable.

5.3.3.4. Contracts with service providers must include logging and monitoring requirements consistent with this policy and rights to access logs for audit and investigation purposes.

5.3.4. AUDIT AND LOGGING PROCESSES

5.3.4.1. This process is intended to provide operational guidance for implementing, monitoring and reviewing audit logs for systems containing personal information, data derived from personal information and non-personal data.

STEP 1: Identify and Classify Systems

5.3.4.2. Identify systems containing personal information, data derived from personal information and non-personal data.

5.3.4.3. Classify systems based on the information security classification of the information in the system.

STEP 2: Configure or Confirm Logging

5.3.4.4. Confirm or Enable logging for user authentication events, data access and changes, administrative actions, ensuring logs capture user ID, timestamp, activity performed and data accessed.

STEP 3: Establish Log Storage

5.3.4.5. Store logs in centralized logging system, if available or at minimum, secure system-specific repositories.

5.3.4.6. Evaluate protections on logs to ensure encryption at rest and in transit and access restrictions.

STEP 4: Define Monitoring Protocols

5.3.4.7. Implement automated monitoring tools where possible.

5.3.4.8. Configure alerts for unusual access patterns, privileged account activity, failed login thresholds.

5.3.4.9. Assign responsibility for monitoring.

STEP 5: Conduct Regular Reviews and Investigate Anomalies

5.3.4.10. Perform periodic reviews in accordance with classification of system. For systems containing restricted information, monthly review is required, while confidential information required quarterly reviews.

5.3.4.11. Document review date, reviewer, finding and action taken.

5.3.4.12. When suspicious activity is detected, escalate to the PAO and IT Security if required. Preserve relevant logs, initiate the privacy breach response process and document findings.

5.4. Security in Contracting

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

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

5.4.3. 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 Cochrane.

5.4.4. 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 provisions in addition to the Privacy, Access and Security policies should be made available to Cochrane upon request, including any updates or revisions that occur after execution of the contract.

5.4.5. All employees of contracted service providers who have exposure to personal information and use Cochrane information assets and systems sign a Confidentiality Agreement. Contracted service providers should remind their employees on termination of their continued responsibility to maintain the confidentiality of Cochrane information.

5.4.6. Contracted service providers immediately report breaches of confidentiality and privacy to the Cochrane PAO.

5.4.7. Contracts with service providers that have access to Cochrane information assets and systems include provisions that protect Cochrane 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 Cochrane.

5.4.8. Contracts with service providers include provisions for destroying or returning all Cochrane 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.

5.4.9. To ensure compliance with contracted provisions for information security, Cochrane:

a) Requests contractors sign an acknowledgement that they have received, read, and will comply with any Cochrane 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.

5.4.10. Cochrane retains the right to inspect the premises and security practices of contracted service providers to ensure compliance with contract provisions and stated policies.

5.4.11. Cochrane avoids using service providers that require the storage or transmission of personal information outside of Canada. If they are retained, Cochrane 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.

6. PRIVACY BREACH RESPONSE

A Privacy Breach (breach) is an unauthorized disclosure, use, destruction, loss, removal, or modification of information in the custody or control of Cochrane. 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.

6.1. Determining Level of Response

6.1.1. 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:

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

b) the internal and external scope and scale of the breach;

c) the known relationship of the recipients to subject individuals; or

d) the intentionality of the cause.

6.1.2. 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.

6.2. Investigation Principles

6.2.1. Cochrane 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:

a) keep investigation information confidential to protect the privacy of individuals investigated and to maintain the integrity of the investigation;

b) use surveillance or monitoring data to establish past or current actions on an as-needed basis

c) examine or confirm the veracity of facts or statements, sometimes using third party witnesses

d) 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;

e) base findings and conclusions on balance of probabilities.

6.2.2. 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.

6.3. Identifying and Reporting Breach

STEP 1: IDENTIFICATION AND REPORTING

6.3.1 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 (Appendix 8.2). If unable to determine the level of the breach, contact the PAO immediately.

6.3.2 The PAO will open and document the breach recording all information required below, including the initial facts of the breach as far as possible within the timelines available:

a) dates of breach and report

b) responsive actions taken so far

c) nature of the 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 breach has been discovered, determine the level of the incident according to Privacy Breach Procedures Table (Appendix 8.2). The highest level where any one of the classes and characteristics apply is the identified Level of the breach.

Level 1 Low:

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

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.

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

Level 2 High:

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

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.

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

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

Level 3 Critical:

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

CONTAINING THE BREACH

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

REPORTING

6.3.4 Depending on the level and nature of the breach, IT, Cochrane leadership and the police are informed.

STEP 3: NOTIFICATION

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

6.3.5 Cochrane informs the Office of the Information and Privacy Commissioner of Alberta 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.

6.3.6 Level 1 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

6.3.7 Cochrane 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.

6.3.8 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

6.3.9 Establish and confirm:

a) dates of breach and report
b) responsive actions taken so far
c) nature of the 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

6.3.10 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 (Appendix 8.2).

FINDINGS

6.3.11 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.

REPORT DISTRIBUTION

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

6.3.13 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 Cochrane Collection, Use, Disclosure and Right of Access policies.

STEP 5: REMEDIATION AND PREVENTION

REMEDIATION

6.3.14 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 need to be tracked.

PREVENTION RECOMMENDATIONS

6.3.15 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.

DISCIPLINE

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

7. RELATED INFORMATION

7.1. Guiding Legislation

7.1.1. Province of Alberta Protection of Privacy Act, SA 2024, Chapter P-28.5

7.1.2. Province of Alberta Protection of Privacy (Ministerial) Regulation 143/2025
7.1.3. Province of Alberta Protection of Privacy Regulation 132/2025
7.1.4. Province of Alberta Access to Information Act, SA 2024, Chapter A-1.4
7.1.5. Province of Alberta Access to Information Act Regulation 133/2025

8. APPENDICES

8.1. 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

8.2. Privacy Breach Response Procedures Table

Level	Severity Criteria		Time from Detection	Response	Responsibility
	Class	Breach Characteristics (if any apply)			
1 Low	I C C C	Internal and external Internal Subject individuals not known to unauthorized recipient Cause of breach was unintentional	2 hrs.	*Step 1:* Report to Manager, PAO	Employee or Service Provider
			24 hrs.	*Step 2:* 1) Confirm breach status 2) Contain breach/retrieve information 3) IT incident, inform IT leadership 4) Confirm requirement for notifications to OIPC, GoA, and subject individual(s)	PAO, Employee or Service Provider, IT, HR
				Step 3: If required: 1) Notify OIPC, GoA 2) Notify subject individual(s)	PAO
			20 days	*Step 4:* Investigate Investigative report to: 1) Leadership 2) IT, if applicable 3) HR, if applicable	PAO
			TBD	*Step 5:* Remediation and Prevention	PAO, Employee or Service Provider, Leadership IT, HR
2 High	C C C R	External Subject individuals likely known to unauthorized recipient Cause of breach intentional Internal	1 hr.	*Step 1:* Report to Manager, PAO	Employee or Service Provider
			3 hrs.	*Step 2:* 1) Confirm breach 2) Contain breach/retrieve information 3) IT incident, inform IT leadership 4) Inform Leadership, Communications 5) Inform Police on potential criminal or public safety concerns 6) Inform HR, if applicable	PAO, Leadership, Employee or Service Provider, IT, HR
			24 hrs.	*Step 3:* 1) Notify OIPC, GoA 2) Notify subject individual(s)	PAO

Level	Severity Criteria		Time from Detection	Response	Responsibility
	Class	Breach Characteristics (if any apply)			
			7 days	*Step 4*: Investigate Investigative report to: 1) Leadership, Communications 2) IT, if applicable 3) HR, if applicable 4) Police, if required 5) OIPC, if required 6) Subject individual(s) on basic findings (not full report)	PAO
			TBD	*Step 5:* Remediation and Prevention	PAO, Employee or Service Provider, Leadership IT, HR
3 **Critical**	R	External	Immediately	*Step 1:* Report to Manager, PAO	Employee or Service Provider
			1 hr.	*Step 2*: 1) Confirm breach 2) Contain breach/retrieve information 3) Inform Leadership, Communications 4) IT Breach, inform IT leadership 5) Inform Police on potential criminal or public safety concerns 6) Inform HR, if applicable 7) Inform high risk subject individual(s)	PAO, Leadership, Employee or Service Provider, IT, HR
			1 hr.	*Step 3:* 1) Notify, consult with OIPC on response 2) Notify remaining subject individual(s)	PAO
			3 days	*Step 4*: Investigate/cooperate with Police and OIPC Investigative report to: 1) Leadership, Communications 2) OIPC, if required 3) Police, if required 4) IT, if applicable 5) HR, if applicable 6) Subject individual(s) on basic findings (not full report)	PAO
			TBD	*Step 5*: Remediation and Prevention	PAO, Employee or Service Provider, Leadership IT, HR

9. End of Policy

Manager, Legislative Services

Mayor

Department: Legislative Services		**Responsible Officer: Manager, Legislative Services**	
Date modified	**Scheduled review date**	**Approval authority**	**Summary of changes from the previous version**
06/08/26	Q2 2029	Council	New Policy