MUNICIPAL DISTRICT OF SPIRIT RIVER NO. 133 **PRIVACY, ACCESS AND SECURITY POLICY**	**Function/Department:** **Policy No.**	**INFORMATION MANAGEMENT** **IM.01**
	Status:	**Adopted**
	Approval Date:	**October 14, 2026**
	Current Resolution No:	**Motion 451.10.14.26**
	Original Adoption Date:	**October 14th, 2026**
	Action:	***New***

Table of Contents

I. GENERAL PROGRAM POLICY 3

A. PURPOSE 4
B. SCOPE 4
C. GOALS AND PRINCIPLES 4
D. QUALITY CONTROLS AND ASSURANCE 5
E. TERMS AND DEFINITIONS 7
F. ROLES AND RESPONSIBILITIES 12

II. COLLECTION, USE, DISCLOSURE, DATA MATCHING, AND NON-PERSONAL DATA 15

A. POLICY 15
B. PROCESSES 19
C. ARTIFICIAL INTELLIGENCE 21

III. RIGHT OF ACCESS AND CORRECTION OF INFORMATION 25

A. POLICY 25
B. PROCESSES 28

IV. COMPLAINT RESOLUTION 33

A. POLICY 33
B. PROCESSES 34

V. INFORMATION SECURITY 36

A. SAFEGUARDS 36
B. INFORMATION SECURITY CLASSIFICATIONS 38
C. AUDIT LOGGING 39
D. SECURITY IN CONTRACTING 41

VI. PRIVACY BREACH RESPONSE 43

A. POLICY 43
B. PROCESSES 44

APPENDIX 1: FEE SCHEDULE **48**
APPENDIX 2: RESEARCH PROPOSAL FORM **49**
APPENDIX 3: RESEARCH AGREEMENT FORM **55**
APPENDIX 4: CONSENT FORM **57**
APPENDIX 5: SERVICE PROVIDER AGREEMENT **58**
APPENDIX 6: SERVICE PROVIDER CONTRACT PRIVACY CHECKLIST **65**
APPENDIX 7: UNREASONABLE INVASION OF PRIVACY GUIDELINES **72**
APPENDIX 8: DELEGATION ORDER **74**
APPENDIX 9: INFORMATION SECURITY CLASSIFICATION AND STANDARDS TABLE **76**
APPENDIX 10: PHYSICAL SECURITY ZONES REQUIREMENTS TABLE **78**
APPENDIX 11: NETWORK SECURITY ZONES REQUIREMENTS TABLE **79**
APPENDIX 12: PRIVACY BREACH RESPONSE PROCEDURES TABLE **80**
APPENDIX 13: PRIVACY BREACH RESPONSE FORM **82**
APPENDIX 14: COMPLAINT SUBMISSION FORM **87**
APPENDIX 15: COMPLAINT RESPONSE LETTER **89**
APPENDIX 16: SAMPLE COLLECTION NOTICE **91**

I. General Program Policy

PREAMBLE

This Privacy Policy applies to all information under the custody and control of the public body, as well as all individuals defined as "employees" under applicable privacy legislation.

Definition of Employee & Board Member Coverage: In accordance with legislation, an "employee" includes any person performing a service for the public body as an appointee, volunteer, student, contractor, or agent.
Board Members: Because board members are appointed (rather than elected) to perform services on behalf of the public body, they fall under the statutory definition of "employee." Consequently, board members are fully subject to all terms, administrative rules, and enforcement mechanisms contained within the Information Management Policy IM.01.

Responsibility: it is the responsibility of any employee or anyone in custody of any public body information to protect the privacy of individual citizens and its employees.

Application to Elected Officials (Council)

- Governance Distinction: Elected officials (Council) are explicitly excluded from the statutory definition of "employee." Administration and Council operate as distinct bodies: Council governs, while Administration operationalizes. Administrative policies do not directly govern Council members, and employee-specific provisions (such as internal disciplinary consequences) do not apply to them. Council sets its own operational rules and standards through separate governance instruments (e.g., Bylaws, Codes of Conduct).
- Information Handling Rules: While individual Council members are not subject to employee personnel policies, all public body information remains strictly governed by privacy legislation and this policy. Any public body information that Council members access, use, or disclose must be handled in full compliance with the privacy parameters outlined in this policy.

A. PURPOSE

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. MD of Spirit River No. 133 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 MD of Spirit River information in compliance with ATIA and POPA.

B. SCOPE

This policy applies to:

1.1 MD of Spirit River employees, including directors, officers, contractors, students, and volunteers providing services on behalf of MD of Spirit River;

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

1.3 All facilities and equipment required to collect, manipulate, transport, transmit, or keep MD of Spirit River information.

C. GOALS AND PRINCIPLES

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

1. PROGRAM ACCOUNTABILITY

MD of Spirit River 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 MD of Spirit River.

2. OPENNESS

MD of Spirit River develops and follows access, privacy and security policies and practices that are compliant with legislation. Such policies and practices are publicly available.

3. COLLECTION OF PERSONAL INFORMATION

MD of Spirit River 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.

4. IDENTIFYING PURPOSES

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

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.

6. ACCURACY

MD of Spirit River makes all reasonable efforts to ensure that both general information and personal information created or received by MD of Spirit River 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.

7. RIGHT OF ACCESS

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

8. SAFEGUARDS

MD of Spirit River 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.

9. COMPLIANCE CHALLENGES

Individuals are encouraged to bring any concerns or issues regarding privacy and access at MD of Spirit River 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 MD of Spirit River right of access or correction responses, or any policies or practices that they feel are not in compliance with legislative requirements.

D. QUALITY CONTROLS AND ASSURANCE

1. POLICY REVIEW AND ASSESSMENT

1.1 MD of Spirit River reviews and assesses Privacy, Access and Security policies every four years to ensure that they are effective and align with legislative, regulatory or MD of Spirit River functional developments and changes. Policies may be reviewed outside the regular review period if organizational or legislative changes necessitate it.

2. TRAINING AND COMMUNICATION

2.1 All MD of Spirit River employees and Council members 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 provided when employees are hired and is ongoing and refreshed or expanded upon in regular intervals in accordance with the roles and responsibilities of employees. Frontline staff will refresh training every four years and administrative staff will refresh training every two years. Council members will receive training immediately following election. Board Members will receive training immediately following appointment.

2.2 Training resources are reviewed every four years to ensure that they are effective and align with legislative, regulatory or MD of Spirit River functional developments and changes.

3. PRIVACY, ACCESS, AND SECURITY MONITORING AND ASSESSMENT

3.1 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 MD of Spirit River information are identified, monitored and assessed to determine the extent of the risk and the mitigation required.

3.2 MD of Spirit River has established 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.

4. PERSONAL INFORMATION INVENTORY AND PERSONAL INFORMATION BANKS

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

4.2 A personal information inventory is a comprehensive list of all personal information held by MD of Spirit River. It includes data storage locations, categories of personal information, categories of individuals 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.

4.3 MD of Spirit River creates and maintains a directory of the personal information banks under its custody and control.

4.4 MD of Spirit River publishes the directory of its personal information banks, either in printed or electronic form, and makes it available to the public.

4.5 The personal information bank directory includes:

a) the title of the personal information bank;

b) the location of the personal information bank;

c) a description of the types of personal information included;

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

e) the authority for collecting the personal information;

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

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

4.6 If personal information is used or disclosed for a purpose other than the one described in the directory, MD of Spirit River

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

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

5. PRIVACY IMPACT ASSESSMENTS

5.1 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.

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

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

b) it involves highly sensitive information;

c) it involves personal information of a significant percentage of the MD of Spirit River's service population;

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

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

f) the technology used is innovative; or

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

5.3 Any projects or changes of such nature are reported to the Privacy and Access Officer, who is responsible for completing the PIA.

5.4 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.

E. TERMS AND DEFINITIONS

AI Inference

The process by which a trained AI model takes input data and produces an output, based on conclusions and reasoning.

Artificial Intelligence Service (AI Service)

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.

"ATIA"
The Access to Information Act, SA 2024, cA-14, as amended, from time to time.

Authorized Representative

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 (Appendix 7) of the minor

f) An individual acting with the written authorization of an individual

Collection

To gather, acquire or obtain personal information about an individual, from any source, including third parties.

Common or integrated service or program

A program or service planned, administered, delivered, managed, monitored or evaluated by MD of Spirit River working collaboratively with one or more other public bodies or another public body working on behalf of MD of Spirit River or MD of Spirit River and one or more other public bodies.

Confidentiality

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.

Consent

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.

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 MD of Spirit River has custody of the information. MD of Spirit River 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.

Data Derived from Personal Information

Data created or derived from data matching that identifies individuals whose personal information was used in the data matching process. May include AI Inferences.

Data Matching

Linking of personal information between 2 or more databases or other electronic sources of information.

Disclosure

Giving access to or making the personal information in MD of Spirit River' custody or control available to a person or organization external to MD of Spirit River.

Employee

All employees, including board members, directors, officers, contractors, students, and volunteers providing services on behalf of MD of Spirit River.

External Networked Source

Interconnected computer networks, such as the internet, that contain information for which MD of Spirit River has little to no control over content creation, integrity or disclosure.

High Sensitivity Information

Personal information about an individual that is:

a) Biometric information

b) Financial information

c) Personal information about a minor, senior or vulnerable person

Individual

Any person, living or deceased, regardless of residency, citizenship, or status. In addition, the authorized representative of the individual.

Large Language Model (LLM)

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.

Law Enforcement

Policing, including criminal intelligence operations, security or administrative investigation that leads or could lead to a penalty or sanction.

Mature Minor

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.

Notification

An explanation of policies, procedures, consequences, and risks related to the collection, use or disclosure of an individual's personal or personal employee information. MD of Spirit River 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 MD of Spirit River if an individual has questions about the management of their personal information.

Non-personal Data

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.

Personal Employee Information

Personal information collected, used, or disclosed solely for the purposes of establishing, managing, or terminating an employment or volunteer relationship.

Personal Information

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
p) Individual's personal views or opinions (except opinions about others)

*Home or 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:

a) Opinions contained in work product
b) Classification, salary range, discretionary benefits, or employment responsibilities of public body employees

c) Financial and other details of a contract to supply goods or services to a public body

d) Information about a license, permit, financial or other discretionary benefit granted to an individual by a public body

e) Information is about an individual who has been dead for 25 years or more

f) 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

Personal Information Bank (PIB)

An information repository that is organized or retrievable by an individual's name or other identifier.

Privacy Impact Assessment (PIA)

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.

Privacy Officer

The municipality staff member(s) designated as Privacy Officer(s) by the Chief Administrative Officer in accordance with the *Chief Administrative Officer Bylaw* and Section 209 of the *Municipal Government Act.*

Prompt

A cue, instruction, or question given to an AI Service to elicit a response, action, or creative output.

Reasonable Security Arrangements

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 MD of Spirit River 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 an individual who is the subject of non-personal data cannot be re-identified from the data.

Record

Information in any form, including 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.

Research

Academic, applied, or scientific research, excluding internal program or quality improvement assessments, that necessitates the use of individually identifying personal information.

Severing

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.

Significant Harm

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
i) Loss of finances

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

a) It is reasonably believed that the information has been or will be misused
b) The unauthorized access, disclosure of loss was the result of malicious intent
c) The personal information is sensitive
d) Existing mitigating factors reduce the risk of significant harm

Third Party

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 MD of Spirit River.

Use

Use of information by MD of Spirit River employees for an authorized purpose that is authorized by policy or law.

F. ROLES AND RESPONSIBILITIES

1. HEAD

1.1 Unless otherwise delegated, the Head of MD of Spirit River is responsible for all obligations and discretionary decision-making under ATIA and POPA.

1.2 The Head of MD of Spirit River is recognized as the CAO.

1.3 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 F.2, below.

1.4 The Head is responsible for ensuring that privacy, access and security policy and practices in the MD of Spirit River are aligned with governing mandates, standards, and planning.

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 MD of Spirit River in accordance with the delegation order (Appendix 8). The PAO is responsible for 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) Developing and completing quality assurance processes for implementation of MD of Spirit River organization privacy and access management.

c) Providing training and resources so that MD of Spirit River 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 MD of Spirit River in dealings with third parties, the provincial government, and the Office of the Privacy Commissioner of Alberta, as necessary.

RIGHT OF ACCESS, CORRECTION, AND COMPLAINTS

e) 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.

f) Responding to request for correction of personal information, including, as necessary, transfer of requests, correcting personal information, annotating personal information, notifying recipients.

g) 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.

PRIVACY AND SECURITY

h) In consultation with MD of Spirit River employees, providing advice, interpretation and implementation of applicable legislation regarding personal information, including release / non-release, collection, use and disclosure of personal information.

i) Maintaining the security, protection and accuracy of personal information in the custody or control of MD of Spirit River in compliance with legislation and policy.

j) Directing the response to privacy breaches of personal information at MD of Spirit River and its facilities in line with legislation and the Privacy Breach Response Policy.

k) Completing Privacy Impact Assessments (PIAs) for MD of Spirit River for project-specific personal information systems and practices.

l) 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.

3. INFORMATION TECHNOLOGY MANAGEMENT

IT Management, in coordination with the PAO, for all systems, networks and applications:

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.

4. 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 PAO;

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 PAO;

g) reports any new information repositories or data systems that require registration, assessment, and security classification to the PAO.

5. ALL MD OF SPIRIT RIVER EMPLOYEES AND SERVICE PROVIDERS

All MD of Spirit River 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.

Responsibility: it is the responsibility of any employee or *anyone in custody of any public body information* to protect the privacy of individual citizens and its employees.

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 PAO all decisions about collection, use, disclosure, and access that are not clearly directed by policy;

f) report all suspected breaches to personal information to the PAO immediately upon discovery;

g) identify and report information security incidents to the appropriate management according to privacy breach procedures.

Collection, Use, Disclosure, Data Matching, and Non-Personal Data

G. POLICY

1. COLLECTION OF PERSONAL INFORMATION

1.1 MD of Spirit River 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.

1.2 MD of Spirit River collects personal information directly from the individual, or their authorized representative. MD of Spirit River 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 MD of Spirit River 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 MD of Spirit River;

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 MD of Spirit River;

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 MD of Spirit River personnel;

o) the personal information is required to support researching or validating claims, disputes, or grievances of aboriginal people;

p) the personal information is required to plan, manage, deliver, monitor and evaluate a common or integrated program or service.

1.3 When collecting personal information directly from an individual, MD of Spirit River 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.

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.

1.5 MD of Spirit River employees collect only the amount and types of personal information as required to complete the stated function or purpose.

2. CONSISTENT PURPOSES

2.1 MD of Spirit River will primarily use and disclose personal information for the purpose for which it was originally collected or for a consistent purpose.

2.2 For a use or disclosure to be for a consistent purpose, MD of Spirit River 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 MD of Spirit River.

2.3 In assessing the consistent purpose, MD of Spirit River 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.

3. USE OF PERSONAL INFORMATION

3.1 MD of Spirit River 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 MD of Spirit River by another public body, under the allowable disclosure provisions.

3.2 MD of Spirit River employees use only the amount and types of personal information as required to complete the state function or purpose.

4. DISCLOSURE OF PERSONAL INFORMATION

4.1 MD of Spirit River may disclose personal information for the purpose for which the information was collected or compiled or for a purpose consistent with that purpose;

4.2 MD of Spirit River 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);

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 MD of Spirit River if necessary for their duties;

n) to an officer or employee 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 MD of Spirit River 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.

4.3 MD of Spirit River employees disclose only the amount and types of personal information as required to perform their assigned duties.

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.

4.5 MD of Spirit River will not sell personal information under its custody or control in any circumstance or for any purpose.

5. RESEARCH DISCLOSURE

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 OIPC;

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) MD of Spirit River 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 (Appendices 2 and 3).

6. DATA MATCHING AND NON-PERSONAL DATA

6.1 MD of Spirit River

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.

6.2 For the purposes of data matching, MD of Spirit River:

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.

6.3 MD of Spirit River 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.

6.4 MD of Spirit River 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 MD of Spirit River to carry out that purpose.

6.5 MD of Spirit River 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.

6.6 MD of Spirit River 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.

6.7 MD of Spirit River is not restricted from disclosing reports, summaries or other publications containing non-personal data that is aggregate or statistical form.

H. PROCESSES

1. CONSENT STANDARDS

1.1 MD of Spirit River can only request the consent of the individual for use or disclosure of their personal information, not for collection.

1.2 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.

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

1.4 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.

1.5 MD of Spirit River accepts oral consent for the following purposes:

a) an individual is unable to submit manual or electronic means of consent or attend MD of Spirit River offices in person.

1.6 MD of Spirit River communicates that it accepts consent provided orally for the purposes specified above.

1.7 MD of Spirit River authenticates the identity of the individual providing the oral consent. MD of Spirit River ensures that the method of authentication is reliable for verifying the identity of the individual and for associating the consent with the individual.

1.8 When oral consent is used, MD of Spirit River ensures that a record of the consent is created, is retained by MD of Spirit River, and is accessible for subsequent reference. A record of consent may include audio or video recording, or written notes from the person administering the process.

2. RESEARCH PROJECT AGREEMENTS

2.1 Researchers are required to submit a Research Proposal (Appendix 2) for consideration and approval by the PAO.

2.2 MD of Spirit River discloses personal information for research purposes only if the recipient signs an agreement (Appendix 3).

3. NON-PERSONAL DATA BEST PRACTICES AND REQUIREMENTS

3.1 MD of Spirit River 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.

3.2 When creating non-personal data, and before it is used or disclosed, MD of Spirit River:

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.

3.3 MD of Spirit River assesses and records the risk and mitigations of risks of its de-identification standards and techniques resulting in re-identification. As part of this assessment MD of Spirit River 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.

3.4 Whenever non-personal data is created from personal information under its custody or control, and before it is used or MD of Spirit River 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.

I. ARTIFICIAL INTELLIGENCE

1. COLLECTION, USE AND DISCLOSURE

1.1 When MD of Spirit River 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) MD of Spirit River considers information about individuals extracted by an AI service from external networked sources, including the internet, as personal information.

h) MD of Spirit River 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) MD of Spirit River considers inferences generated by an AI service containing personal information as data derived from personal information.

2. INFORMATION ACCURACY AND INTEGRITY

2.1 MD of Spirit River 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.

2.2 Inferences generated by AI services for MD of Spirit River use include citations and references to sources detailed enough to verify the veracity and completeness of the information.

3. NOTIFICATION

3.1 MD of Spirit River 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.

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.

3.3 Upon request, MD of Spirit River 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.

3.4 This notification may not be provided in cases where one of the circumstances or conditions which require or allow MD of Spirit River to withhold the information apply.

4. REGULATION OF USE

4.1 MD of Spirit River controls and regulates the use of AI for specified purposes based on the risk to individuals.

4.2 MD of Spirit River 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.

4.3 MD of Spirit River employees complete high-risk AI activities only with the approval of the PAO, who evaluates the risk on a case-by-case basis.

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

4.5 MD of Spirit River 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.

4.6 MD of Spirit River employees complete low-risk AI activities as required based on their effectiveness for the purpose.

4.7 Where practical and effective for purpose, MD of Spirit River 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.

II. 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 MD of Spirit River. 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.

A. POLICY

1. RECEIVING AND FACILITATING REQUESTS

1.1 Requests for access to MD of Spirit River 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.

1.2 MD of Spirit River 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.

1.3 MD of Spirit River does not deny access to information based on the applicant's reason or purpose for the request.

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

1.5 Once the applicant has met the requirements to make a request, MD of Spirit River 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.

2. EXCLUDED RECORDS

2.1 Some records that are in the custody or control of MD of Spirit River are excluded from the ATIA and do not have to be considered relevant or released as part of a right of access request. However, MD of Spirit River may choose to release this information as part of a request under specified circumstances. Excluded records include:

a) Records designated by MD of Spirit River 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) MD of Spirit River 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 MD of Spirit River;

h) Health records created or received by a MD of Spirit River doctor or nurse;

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

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

j) Records from private sector donors that are preserved in MD of Spirit River archives for historical research purposes.

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

3. DISREGARDING REQUESTS

3.1 MD of Spirit River 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 MD of Spirit River 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.

3.2 The applicant is informed of the reasons for disregarding the request and the right to ask the Commissioner to review MD of Spirit River's decision.

4. SEARCHES FOR RELEVANT RECORDS

4.1 MD of Spirit River 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 MD of Spirit River, that was created or received by employees and contractors to support their functions as MD of Spirit River officials.

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 the public body.

4.3 MD of Spirit River 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.

5. REVIEWING AND WITHHOLDING INFORMATION

5.1 MD of Spirit River 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.

5.2 MD of Spirit River 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.

5.3 MD of Spirit River 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, recommendations, analyses or policy options developed by or for the public body;

h) cause harm to the economic interests of MD of Spirit River 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.

6. PUBLIC HEALTH AND SAFETY OVERRIDE

6.1 MD of Spirit River discloses without delay, to the public, a group of people, an individual, or an applicant, any information that MD of Spirit River 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.

6.2 Before disclosing the information MD of Spirit River 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.

7. THIRD PARTY REVIEWS

7.1 MD of Spirit River 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.

8. REQUESTS FOR CORRECTION OR AMENDMENT OF PERSONAL INFORMATION

8.1 Individuals may request correction or amendment of their own personal information in the custody or control of MD of Spirit River.

8.2 MD of Spirit River will not amend professional opinions that are made by employees that have the competency to make them.

B. PROCESSES

1. RIGHT OF ACCESS INTAKE

1.1 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.

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

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

1.4 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.

1.5 The Privacy and Access Officer 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.

1.6 The Privacy and Access Officer 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 Officer requests further detail and clarification, the applicant must respond within 30 business days or the request will be considered abandoned.

1.7 Within 15 business days after MD of Spirit River receives a request, the Privacy and Access Officer may transfer the request and if necessary, the record to another public body if the record was produced by or for the other public body, the other public body was the first to obtain the record or the record is in the custody or control of the other public body. The Privacy and Access Officer will notify the applicant of the transfer.

2. FEES

2.1 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 1).

2.2 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.

2.3 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.

2.4 The Privacy and Access Officer 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.

2.5 If the applicant requests a waiver of fees, the Privacy and Access Officer 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 Officer responds to a request for waiver of fees within 30 business days.

2.6 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.

2.7 Regardless of the fee estimate, MD of Spirit River only charges fees beyond the initial administrative fee that reflect the actual costs incurred.

3. RETRIEVAL AND REVIEW OF RELEVANT RECORDS

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

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

3.3 The Privacy and Access Officer 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.

4. THIRD PARTY REVIEWS

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

4.2 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 Officer to either disclose the information or explain why the information should not be disclosed.

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

4.4 The Privacy and Access Officer 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.

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

4.6 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.

5. RESPONSE TO APPLICANT

5.1 Having completed a review of the records, the Privacy and Access Officer 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.

5.2 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.

5.3 Requested information will be provided in a form that is generally understandable. MD of Spirit River 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.

5.4 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.

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

6. TIME LIMITS FOR RESPONDING TO A REQUEST

6.1 MD of Spirit River responds to right of access requests within 30 business days of the receipt of the request.

6.2 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 MD of Spirit River decision to waive of fees.

6.3 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;

6.4 If the response time is extended, the Privacy and Access Officer 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.

6.5 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 Officer notifies the Commissioner as soon as possible of the operational closure, the anticipated re-opening, and when the re-opening occurs.

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

7. CORRECTION OR AMENDMENT REQUEST PROCESSES

7.1 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.

7.2 MD of Spirit River 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.

7.3 Formal requests to correct or amend information subject to review must be in writing to the MD of Spirit River Privacy and Access Officer. 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.

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

7.5 MD of Spirit River responds to formal requests for correction of personal information within thirty (30) business days of receipt of the request.

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

7.7 MD of Spirit River 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 MD of Spirit River's decision.

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

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

8. INDIVIDUAL CHALLENGES TO REQUEST RESPONSES

8.1 Individuals are encouraged to bring any concerns or issues concerning responses to requests and compliance with this policy 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.

III. Complaint Resolution

A. POLICY

1. SUBMISSION

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

1.2 Complaints may concern any decision, act, or failure to act by MD of Spirit River in a formal access to information request or in the protection of personal information, data derived from personal information, and non-personal data under MD of Spirit River's custody or control or by a MD of Spirit River 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 MD of Spirit River 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.

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.

2. PRINCIPLES OF INVESTIGATION AND RESPONSE

2.1 The Privacy and Access Officer receives, processes, investigates, and responds to complaints under ATIA and POPA made to MD of Spirit River.

2.2 If an investigation is required to establish findings for a complaint, MD of Spirit River 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.

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.

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.

3. RESPONSE

3.1 MD of Spirit River 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.

3.2 MD of Spirit River provides responses in writing, containing the findings of the Privacy and Access Officer, to all formal complaint submissions.

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

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 Officer 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.

B. PROCESSES

1. RECEIVING SUBMISSIONS

1.1 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 (Appendix 14):

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.

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

2. ACKNOWLEDGE RECEIPT OF SUBMISSION

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

3. INVESTIGATION AND ANALYSIS

3.1 The Privacy and Access Officer determines the scope and nature of the complaint according to the parameters established in section IV.A.1.3 and records the investigation scope as part of the complaint investigation file.

3.2 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.

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

3.4 The Privacy and Access Officer 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.

3.5 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. FINAL RESPONSE

4.1 When the findings of the investigation are determined, a final written response (Appendix 15) will be provided to the complainant according to the parameters set out in section IV.A.3.

4.2 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.

5. RESOLUTION

REMEDIATION AND PREVENTION

5.1 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 MD of Spirit River systems, processes, and employee behaviours. This may include employee or user training, introduction of additional security technology, or upgrade to facilities or infrastructure.

IV. Information Security

The information security provisions of POPA require MD of Spirit River 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 MD of Spirit River to protect confidential information.

A. SAFEGUARDS

1. ADMINISTRATIVE

1.1 MD of Spirit River ensures that policies and procedures to facilitate the safeguarding of confidential information in its custody or control are developed and maintained.

1.2 The need for confidentiality and security of personal information is addressed as part of the conditions of employment for MD of Spirit River 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.

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

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.

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, MD of Spirit River completes a Privacy Impact Assessment (PIA) that describes how the new initiative will affect privacy, and what measures MD of Spirit River will put in place to mitigate risks to privacy.

1.6 An agreement or contract (Appendix 5) is completed and signed between MD of Spirit River and all contracted service providers that require access to the information systems and assets of MD of Spirit River that requires that they meet or exceed MD of Spirit River privacy program standards and policies.

1.7 MD of Spirit River employees and persons acting on behalf of MD of Spirit River report all violations and breaches of information security as soon as possible to MD of Spirit River'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.

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 by-laws and schedules of MD of Spirit River.

2. PHYSICAL

2.1 All MD of Spirit River records, both on-site and off-site, are held and stored in an organized, safe, and secure manner in accordance with information security standards.

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

2.3 MD of Spirit River'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.

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.

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

2.6 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.

2.7 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 MD of Spirit River has ended.

2.8 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.

2.9 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.

2.10 MD of Spirit River employees will verify the identity and credentials of courier services used for the transportation of personal information.

2.11 Printers that may be used to print confidential information are located in a secure area. Employees use the "safe print" feature 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 MD of Spirit River'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.

2.12 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 drives, diskettes, tapes, CD-ROMS, etc.), or the device(s) will be destroyed.

3. TECHNICAL

3.1 Firewalls, intrusion detection software, or other technical means to protect internal MD of Spirit River networks carrying identifiable personal information is in place to prevent unauthorized use and malicious software.

3.2 Access to data and application systems to personal information is limited by each MD of Spirit River 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.

3.3 Employees of MD of Spirit River 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.

3.4 Access to MD of Spirit River 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.

3.5 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).

3.6 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.

3.7 MD of Spirit River do not use service providers, including cloud services, that require the storage of personal information outside of Canada.

3.8 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.

3.9 MD of Spirit River monitors AI services and applications to ensure that there is no leakage of internal inferences and other information to external parties.

B. INFORMATION SECURITY CLASSIFICATIONS

1. CLASSIFICATION LEVELS AND ASSIGNMENT

1.1 Information is classified according to the degree of harm that may result from unauthorized access, loss, or modification. All information is classified in accordance with

the levels identified in the Information Security Classification and Standards Table (Appendix 9) as:

a) Restricted

b) Confidential

c) Internal

d) Public

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

2. SECURITY ZONES

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.

2.2 MD of Spirit River maintains 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 (Appendix 10) and the Network Security Zones Requirements Table (Appendix 11) provide details of standards required for each zone.

C. AUDIT LOGGING

1. LOGGING REQUIREMENTS

1.1 MD of Spirit River 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

2. MONITORING AND REVIEW

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

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.

3. LOG RETENTION AND SECURITY

3.1 Audit logs are retained in accordance with applicable MD of Spirit River retention schedules, with a minimum retention period of at least 12 months.

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

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

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.

4. AUDIT AND LOGGING PROCESSES

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

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

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

STEP 2: CONFIGURE OR CONFIRM LOGGING

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

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

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

STEP 4: DEFINE MONITORING PROTOCOLS

4.7 Implement automated monitoring tools where possible.

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

4.9 Assign responsibility for monitoring.

STEP 5: CONDUCT REGULAR REVIEWS AND INVESTIGATE ANOMALIES

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.

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

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.

D. SECURITY IN CONTRACTING

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

1.2 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 (see Appendix 5 and 6), or have equivalent provisions within terms or use, licensing agreements or contract addendums.

1.3 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 MD of Spirit River.

1.4 Information security provisions outlined in contracts with contracted service providers meet or exceed the standards set out in the Privacy, Access and Security policies and procedures. Any related contracted service provider Privacy, Access and Security policies should be made available to

MD of Spirit River upon request, including any updates or revisions that occur after execution of the contract.

1.5 All employees of contracted service providers who have exposure to and use MD of Spirit River information assets and systems sign a Confidentiality Agreement (see Appendix 1). Contracted service provider service providers should remind their employees on termination of their continued responsibility to maintain the confidentiality of MD of Spirit River information.

1.6 Contracted service providers immediately report breaches of confidentiality and privacy to the MD of Spirit River PAO.

1.7 Contracts with service providers that have access to MD of Spirit River information assets and systems include provisions that protect MD of Spirit River 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 MD of Spirit River.

1.8 Contracts with service providers include provisions for destroying or returning all MD of Spirit River 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.

1.9 To ensure compliance with contracted provisions for information security, MD of Spirit River:

a) Requests contractors sign an acknowledgement that they have received, read, and will comply with any MD of Spirit River 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.

1.2 MD of Spirit River retains the right to inspect the premises and security practices of contracted service providers to ensure compliance with contract provisions and stated policies.

1.3 MD of Spirit River avoids using service providers that require the storage or transmission of personal information outside of Canada. If they are retained, MD of Spirit River 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.

V. Privacy Breach Response

A. POLICY

1. DEFINITION

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

2. DETERMINING LEVEL OF RESPONSE

2.1 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.

2.2 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.

3. INVESTIGATION PRINCIPLES

3.1 MD of Spirit River 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.

3.2 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.

B. PROCESSES

STEP 1: IDENTIFYING AND REPORTING BREACH

IDENTIFICATION AND REPORTING

1.1 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 12). If unable to determine the level of the breach, contact the PAO immediately.

1.2 The PAO will open and document the breach using the Privacy Breach Response Form (Appendix 13) and will document the initial facts of the breach as much 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

1.3 When a breach has been discovered, determine the level of the incident according to Privacy Breach Procedures Table (Appendix 12). 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 MD of Spirit River).

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 MD of Spirit River).

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

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

REPORTING

1.5 Depending on the level and nature of the breach, IT, MD of Spirit River leadership and the police are informed.

STEP 3: NOTIFICATION

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

1.6 The MD of Spirit River 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.

1.7 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

1.8 MD of Spirit River 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.

1.9 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

1.10 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

1.11 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 11).

FINDINGS

1.12 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

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

1.14 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 MD of Spirit River Collection, Use, Disclosure and Right of Access policies.

STEP 5: REMEDIATION AND PREVENTION

REMEDIATION

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

PREVENTION RECOMMENDATIONS

1.16 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

1.17 Depending on the nature and significance of the breach, the role of employees involved, and the information security policy in place, MD of Spirit River can take discipline action

against an employee who has violated MD of Spirit River policy or applicable legislation. This will be passed to Leadership and Human Resources for resolution.

Appendix 1: Fee Schedule

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

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

Appendix 2: Research Proposal Form

PROPOSAL

Access to Personal Information for Research or Statistical Purposes

1. Researcher

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

2. Research Project Description

Project Title
Purpose and Objectives of the Project

Records Requested containing Personal Information	**Identifying (Y or N)**	**De-identified (Y or N)**
-		

Duration of Access
Expected period of time during which access to the personal information will be required

Requirement for individually identifying personal information
Explain why identifying personal information is required to achieve the purposes and objectives of the project.

Data-matching
Explain if and how any personal information will be matched or linked with other data sets to create new information. If so, also explain how the data-matching a) is not harmful to subject individuals and b) is clearly in the public interest.

Other project members requiring access to personal information

Records	**Name and Project Role**

3. Privacy and Security

Applications/Platforms

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

Cloud Storage & File Sharing: Storage (Cloud):
Personal information is stored securely within Microsoft; SharePoint/OneDrive/ TEAMS

Transmission: Microsoft Outlook (email), Google Play/ TEAMS Zoom, or secure SFTP servers for file transfers. utilizing localized data centers. Data is transmitted internally and externally via (e.g., TLS-encrypted email / secure API integrations)

Processing & Core processing of personal data occurs within: CATALIS and *Salesforce* - HR/Payroll

Access Platforms:

Authorized personnel access these platforms via requiring Microsoft ID sign in and Multi-Factor Authentication (MFA).

Paper and Microform Format

- Physical Documents: Printed employment contracts, physical sign-in sheets at the front desk, printed medical forms, physical tax documents, Land files.
- Storage Locations: On-site locked filing cabinets in the HR department, MD Storage vault or off-site secure archiving facilities (e.g., Brownlee Building room automatic lock – limited access archival room and South Peace Regional Archives(located in Grande Prairie). Limited personal information exists in paper format, specifically e.g., signed physical contracts, Land files, HR Files, Taxation documents, payroll information.

3. Security Measures

Digital Security Measures

- Technical Controls: All digital platforms utilize encryption at rest and in transit. Continuous security monitoring and automated daily backups are maintained.
- Access Control: Role-Based Access Control ensures only designated HR/Admin staff can view personal data. Multi-Factor Authentication (MFA) and Single Sign-On (SSO). Access is granted on a least-privilege basis
- Encryption: Data is encrypted both at rest (while stored on servers) and in transit (while being sent over the internet, using protocols like HTTPS or TLS).
- Data Loss Prevention (DLP): iCloud back up subscription and back up server located in the building
- No explicit Disaster Recovery Plan in IT agreement – need to investigate

Physical Security Measures (for Paper)

- Physical Controls: Any physical documentation is housed in restricted-access, locked filing cabinets within an alarmed facility. Disposal is handled via certified secure shredding.
- Visitor Logs: Visitors at the Md office are required to sign in at the front office and are directed to a designated waiting area. The MD has restricted physical access to the buildings.
- Lock and Key: paper records kept in in locked rooms; vault or archives rooms – automatic lock , restricted access to rooms and keys and / or cabinets with restricted key/fob access. Employees have limited access and require CAO or secondary senior employee to allow access to archive buildings.
- Secure Destruction: Using a certified third-party shredding services when paper is no longer needed. Outsourced Shred-It Shredding Services to facilitate destruction – completed on a regular basis.

Devices/Locations
List the types and number of electronic devices that will be used to access, store or process the personal information and any restrictions on where and how they will be used. Describe security measures used to secure devices against unauthorized disclosure or loss.
For paper formats, describe the location where the information will be stored and accessed and the measures in place to security the records within the location.

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

Additional Privacy and Security Measures

4. Data Minimization

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

Records	Method	Date

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

Return and/or Destruction of Information
List how and when information will be returned to public body and/or irrevocably destroyed

Records	Return or Destruction	Method	Date

5. Attestation and Approval

By signing this proposal, the Lead Researcher affirms that the information submitted is, to the best of their

knowledge, accurate and complete.	
Signature of Lead Researcher	**Date**
Public Body Review and Approval	
Privacy and Access Officer Signature	**Date**
Functional Area Representatives Signatures *Representatives from functional areas who manage the identified records*	**Date**

Appendix 3: Research Agreement Form

AGREEMENT

Access to Personal Information for Research or Statistical Purposes

BETWEEN:

MD of Spirit River (Organization)

AND

[Name of Researcher] (Researcher)

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

1. Research Proposal

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

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

2. Privacy and Security Conditions

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

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

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

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

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

3. Breach of Agreement

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

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

4. Attestations

_____

Name and Role of Authorized Research Official

_____ _____

Signature Date

Signatures of other project members requiring access to personal information:

_____

Name and Role

_____ _____

Signature Date

_____

Name and Role

_____ _____

Signature Date

_____

Name and Role

_____ _____

Signature Date

_____

Name and Role

_____ _____

Signature Date

SCHEDULE A

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

Appendix 4: Consent Form

CONSENT FOR USE OR DISCLOSURE OF PERSONAL INFORMATION

I, _____, consent to the release of
(Name)

_____, to
(Identify nature of personal information)

_____, for the purpose of
(Identify individual/organization to whom information is released)

_____.
(Indicate why information is being disclosed)

I acknowledge that I have been made aware of the reasons for the use, disclosure of the above information, and the risks and benefits associated with consenting or not consenting to its release.

I understand that I make revoke my consent at any time, by providing a signed, written statement to MD of Spirit River.

Signature: _____ Print Name: _____

Date: _____ Valid until (optional): _____

Appendix 5: Service Provider Agreement

AGREEMENT

Service Provider Access, Privacy and Security

BETWEEN:

(HEREINAFTER REFERRED TO AS 'ORGANIZATION)

AND

(HEREINAFTER REFERRED TO AS 'SERVICE PROVIDER')

1. Principles

1.1 The privacy standards and conditions under which third-party service providers handle ORGANIZATION personal information must comply with privacy legislation to which ORGANIZATION is subject, including the Alberta *Protection of Privacy Act*, the Alberta *Access to Information Act* and their regulations.

1.2 ORGANIZATION maintains adequate
s and accountability for the privacy and security of personal information handled by third-party service providers.

2. Objectives

2.1 The objective of this agreement is to clearly articulate the privacy and security conditions and requirements under which a third-party service provider handles ORGANIZATION personal information in compliance with ORGANIZATION Privacy and Security Policy.

3. Definitions

3.1 *Service Providers*
Agents of ORGANIZATION who:

- process, store, retrieve, or dispose of ORGANIZATION's personal information;
- strip, encode, or otherwise transform individually identifying personal information of ORGANIZATION to create non-identifying personal information; or
- provide information management or information technology services that involve handling of ORGANIZATION's personal information.

3.2 *Information Security Measures*
Equipment, facilities, systems, practices or other technical, administrative and physical security measures that are implemented to protect the confidentiality and integrity of Service Information or any other ORGANIZATION information that may be affected by SERVICE PROVIDER'S access to the Service Information.

3.3 *General Information*
Service information that is not personal information.

3.4 *Personal Information*
Service information that provides information about and identifiable individual.

3.5 *Representatives*
Directors, officers, employees, partners, associates, agents, or other authorized persons of SERVICE PROVIDER.

3.6 *Service Information*
Any and all general or personal information created or received by SERVICE PROVIDER in the course of completing the Services described in 3.5. Service Information includes all such information, whether written, electronic, magnetic or transmitted orally, and any reports, data tables, extracts, notes, analyses, compilations, studies, reproductions or copies.

3.7 *Services*
Services set out in the attached Schedule A and which are provided by SERVICE PROVIDER to ORGANIZATION.

4. ORGANIZATION Ownership and Control of Information

4.1 SERVICE PROVIDER acknowledges and agrees that all Service Information made available to SERVICE PROVIDER is the property and under the control ORGANIZATION and shall remain the sole property of ORGANIZATION.

4.2 SERVICE PROVIDER acknowledges and agrees that the Service Information is being disclosed to SERVICE PROVIDER strictly on a Service basis and under a relationship of utmost confidence and trust.

4.3 SERVICE PROVIDER and ORGANIZATION agree that the collection, use, disclosure, security, storage and disposal of Service Information and all other information exchanged between ORGANIZATION and SERVICE PROVIDER pursuant to this Agreement is subject to privacy legislation and other territorial or federal laws applicable to ORGANIZATION.

5. Business Reasons for Collection, Use, Disclosure, and Correction of Information

5.1 SERVICE PROVIDER shall limit its collection, use, and disclosure, and correction of Service Information that is required to complete the Services. A description of the Service Information that may be required by SERVICE PROVIDER and the business reason for collecting, using, disclosing, and correcting this information is included in Schedule A of this Agreement.

5.2 SERVICE PROVIDER shall not sell Service Information, for any purpose or under any circumstances.

6. Right of Access and Correction of Information

6.1 SERVICE PROVIDER shall notify ORGANIZATION immediately of a request by an individual or organization for access to or correction of Service Information and shall not disclose or attempt to correct Service Information in response to such requests unless specifically instructed by ORGANIZATION to provide access or to correct the information.

7. Compliance with ORGANIZATION Privacy and Security Policy

7.1 SERVICE PROVIDER shall comply with all ORGANIZATION Policies. ORGANIZATION shall provide to SERVICE PROVIDER a copy of all ORGANIZATION Policies to which SERVICE PROVIDER must comply including, but not limited to, ORGANIZATION policies relating to the following:

a) collection, use, and disclosure of ORGANIZATION personal and general information

b) right of access and correction of ORGANIZATION personal and general information

c) Privacy Impact Assessments and information security reviews of ORGANIZATION information and third party handling systems and procedures

d) technical and physical protection of ORGANIZATION information and resources, including:

i) information storage and handling

ii) user access management

iii) system audit controls

iv) network security

v) equipment and media security

vi) information classification, retention, and destruction

vii) systems backup and recovery

viii) information exchange and electronic mail

ix) personnel security and screening

x) information security training of personnel

xi) privacy breach response procedures

7.2 By executing this Agreement, SERVICE PROVIDER acknowledges awareness and understanding of ORGANIZATION Policies. ORGANIZATION shall have the right to amend ORGANIZATION Policies at any time and SERVICE PROVIDER shall comply with such amended ORGANIZATION Policies immediately upon being provided with notice of the amendment.

7.3 Notwithstanding the requirements in 8.1 and 8.2, ORGANIZATION may instead choose to accept all or part of relevant policies and processes of the SERVICE PROVIDER that relate to the privacy and security of services and information described in Schedule A. To meet this requirement, SERVICE PROVIDER must identify and provide copies of SERVICE PROVIDER's policies and/or processes relevant to any of the privacy and security areas listed in 8.2 for review and approval by ORGANIZATION. For any SERVICE PROVIDER policies or process that are not received or approved by ORGANIZATION or do not adequately address the privacy and security areas listed in 8.2, 8.1 and 8.2 shall apply.

8. Information Security Measures

8.1 SERVICE PROVIDER shall use its best efforts to implement all Information Security Measures required to comply with this Agreement. If and when ORGANIZATION believes, acting reasonably,

that SERVICE PROVIDER's and/or Representative's information security measures are deficient and represent an undue risk to the security of the Service Information or other ORGANIZATION information, ORGANIZATION may make a request in writing for SERVICE PROVIDER to change, modify, or add to such measures. Within (5) days of receipt of this request, SERVICE PROVIDER, at its own expense, shall change or modify its Information Security Measures to comply with this request.

9. Access to information

9.1 SERVICE PROVIDER will ensure that its personnel are restricted and monitored to ensure that they access the least amount Service Information required to complete the services for which they are directly responsible.

10. Information Security Breaches

10.1 SERVICE PROVIDER shall notify ORGANIZATION immediately of any breach of information security affecting the service information, including unauthorized disclosure, use, destruction, loss, removal, modification, or interruption in the availability of service information, whether accidental or as the result of a deliberate act. ORGANIZATION will direct and conduct the breach investigation and will have access to any of SERVICE PROVIDER's and/or its Representative's information systems, equipment, facilities, and personnel affecting the Service Information and relevant records required to complete the breach investigation.

11. Reproduction, Return or Destruction of Service Information

11.1 SERVICE PROVIDER and its respective Representatives shall not copy or otherwise reproduce any of the Service Information or part of any of the Service Information, or any reports, extracts, notes, memoranda or other records in respect thereof, without the prior written instruction of ORGANIZATION.

11.2 At any time upon the written request of ORGANIZATION, or at the termination of this contract, SERVICE PROVIDER shall immediately return to ORGANIZATION or shall have destroyed any and all Service Information and shall not retain any copies or other reproductions thereof. All Service Information returned by SERVICE PROVIDER or the Representative to ORGANIZATION must be in a format that is readable and usable by ORGANIZATION. Furthermore, SERVICE PROVIDER shall, upon request, provide written confirmation to ORGANIZATION that the terms and conditions of this section have been complied with.

11.3 SERVICE PROVIDER shall not be entitled to, and hereby waives any and all right to, withhold any Service Information from ORGANIZATION to enforce any alleged payment obligation or in connection with any dispute relating to the terms of the Agreement or any other matter between ORGANIZATION and the Service Provider.

12. Compliance by Representatives

12.1 SERVICE PROVIDER may disclose Service Information to a Representative of SERVICE PROVIDER who has a need to know the Service Information according to the business reasons in Schedule A. SERVICE PROVIDER will implement personnel security and screening for its Representatives to a standard equal to or exceeding those policies and standards in place for ORGANIZATION employees. SERVICE PROVIDER shall, before disclosing any Service Information to any Representative, use its best efforts to ensure that the terms and conditions of this Agreement are and will be fully complied with by any such Representative, including obtaining an agreement in

writing of such Representative that he will keep such Confidential Information in strict confidence and that he shall be bound by all terms and conditions of this Agreement.

12.2 At the request of ORGANIZATION, SERVICE PROVIDER agrees to provide ORGANIZATION with a list of all Representatives to whom Service Information has been provided and evidence that the Representatives have agreed to be bound by the terms and conditions of this Agreement. SERVICE PROVIDER agrees that it shall be liable and responsible for any breach of this Agreement by their respective Representatives.

13. Inspection without Notice

13.1 ORGANIZATION at its discretion shall have the right to make inspections, without notice, of SERVICE PROVIDER's and/or its Representative's information systems, equipment, facilities, affecting the Service Information and relevant records to ensure appropriate technical, administrative, and physical security measures are being taken to protect the Service Information or other ORGANIZATION information in compliance with this agreement.

14. Termination of Access to Service Information

14.1 Except where there is a statutory or legal compulsion to disclose the Service Information, SERVICE PROVIDER agrees that ORGANIZATION is not obligated to provide SERVICE PROVIDER and/or its Representatives with any Service Information. ORGANIZATION shall have the right to cease providing Service Information to SERVICE PROVIDER and/or its Representatives at any time and for any reason.

15. Legal Obligation to Disclose

15.1 If SERVICE PROVIDER or its Representative is or becomes legally compelled, by subpoena, warrant, court order, statutory requests, or other legal process to disclose any of the Service Information, SERVICE PROVIDER shall provide ORGANIZATION with immediate written notice of this compulsion to allow ORGANIZATION to seek a protective order or other appropriate remedy. If such protective order or remedy is not obtained, SERVICE PROVIDER or the Representative shall:

a) provide only that part of the Service Information which is legally required;

b) use its best efforts to assure that the Service Information will be remain secure and confidential; and,

c) immediately provide ORGANIZATION with copies of the request for the Service Information and all Service Information that was disclosed.

16. Indemnity

16.1 SERVICE PROVIDER hereby indemnifies and saves harmless ORGANIZATION and their respective directors, officers, agents, and employees (collectively, the "Indemnified Parties") from and against any and all penalties, fines, liabilities, damages, cost, expenses, causes of action, actions, claims, suits and judgments that the Indemnified Parties may incur or suffer or be put to by reason of or in connection with or arising from any breach of this Agreement or the Act by the SERVICE PROVIDER, its employees or agents.

17. Relationship to other Agreements

17.1 This Agreement is supplementary and in addition to the Contract and any other contractual obligations that may exist between SERVICE PROVIDER and ORGANIZATION can only be amended by agreement in writing executed by the parties.

IN WITNESS WHEREOF the parties hereto have executed this agreement on [date].

ORGANIZATION	***SERVICE PROVIDER***
_____	_____
Signature	Signature
_____	_____
Please print name	Please print name

SCHEDULE A

SERVICES/PURPOSE	SERVICE INFORMATION	PERSONAL INFORMATION ACTIVITY (Y/N)*			
		Collection	***Indirect***	***Use***	***Disclosure***

*For each of the Services/Purposes listed, confirm whether the service provider will be performing any of the following activities with personal information of the organization:

Collection: receiving/creating new personal information
Indirect: collection of personal information from a source other than the subject individuals
Use: viewing/using/sharing personal information already collected within the organization
Disclosure: disclosing/sharing personal information already collected with parties outside of the organization

Appendix 6: Service Provider Contract Privacy Checklist

This Checklist is provided by the Alberta Office of the Information and Privacy Commissioner.

Below is a list of provisions that a public body should consider including in contracts with service providers when the service provider performs a service on behalf of a public body and in doing so has access to personal information subject to the *Protection of Privacy Act* (POPA). The contract should also include provisions regarding an individual's right of access to their own personal information under the *Access to Information Act* (ATIA).

DISCLAIMER: This checklist IS NOT a complete list of contract provisions that are generally in contracts, such as indemnification clauses. The applicability of these clauses depends on the nature of the work of the service provider for the public body and must be customized accordingly. A public body should consult with legal counsel when entering into contracts as a measure of ensuring their legal interests will be met through the contract provisions.

TOPIC	DESCRIPTION	YES	NO (Reason)
Control and Accountability	The contract specifies the relationship between the public body and the service provider as it relates to the services provided and that any collection, use or disclosure of personal information by the service provider on behalf of the public body must only be carried out in accordance with the terms of the contract.		
	"Personal information" is defined in the contract as defined in POPA.		
	The contract specifies that any personal information that is collected, or otherwise generated or used, and that is in the custody of the service provider for the purpose of providing the services to the public body, is in the control of the public body and that POPA and ATIA apply to this information.		
	The contract specifies that as a service provider to the public body, as it relates to the personal information in the custody of the service provider to provide the services, the service provider is bound to comply with POPA and ATIA as an "employee" of the public body.		
	The contract specifies the types of records containing personal information (list them) that the service provider has access to or that it will create as part of performing the services for the public body.		
	The contract requires the service provider to enter into confidentiality agreements with any of its employees who will have access to personal information to perform the services for the public body, which agreement must align with the service provider's duties under the contract as it relates to its handing of the personal information.		

TOPIC	DESCRIPTION	YES	NO (Reason)
	The contract restricts the use of subcontractors to perform any of the services without express written consent of the public body. If said consent is given, the contract requires the contractor to bind, through its contract with any subcontractor, the subcontractor to the terms of the contract between the service provider and public body as it relates to its duties concerning the personal information therein.		
	The contract requires the service provider to comply with the terms of the agreement and as an employee of the public body to ATIA and POPA.		
Control and Accountability	The contract specifies that the service provider is fully and solely responsible for the actions of its employees, subcontractors, and agents who act on its behalf in the performance of its functions under the contract. If applicable, the contract restricts a service provider's ability to subcontract.		
	The service provider has designated in the contract a senior individual within its organization to be the point of contact for complying with privacy and security obligations set out in the contract, and the contract specifies that any privacy and security issues that arise under the contract or for ascertaining compliance with the privacy provisions therein, the public body's Privacy Officer will be involved.		
	The contract clarifies how the service provider would notify the public body of any requests it receives to produce personal information it has in its custody to a government or law enforcement agency outside of Alberta.		
	The contract requires the service provider to provide the public body, upon request, with an up-to date list of all employees, subcontractors, or agents who have access to the personal information for the purposes of providing the services.		
	The contract specifies that any failure of the service provider, or of its employees or subcontractors, to follow the terms relating to the collection, use, disclosure, security or management of the personal information as set out in the contract is considered a breach of the contract.		
	The contract requires the service provider to advise the public body in advance in the event of any change in ownership of all or a part of the contractor's business.		
	The contract requires the service provider to immediately notify the public body in the event of any proceedings for bankruptcy or insolvency brought by or against the contractor under applicable bankruptcy or insolvency laws or any notice of creditor's remedies.		

TOPIC	DESCRIPTION	YES	NO (Reason)
	Audit and inspection of records or personal information The contract specifies when and how the public body will ensure oversight of the requirements in the contract, including that it may require compliance reports from the service provider as specified therein, and may enter the service provider's premises to inspect, audit, or require a third party to audit the service provider's compliance with the privacy, security, and information management requirements under the contract and that the service provider must co-operate with any such audit or inspection.		
	The contract requires the service provider to maintain specific information to enable the conduct of inspections and audits, i.e. the maintenance of some form of audit trail (electronic or paper form) for as long as the public body determines as necessary, and for compliance reporting purposes.		
Legal Authorities for Collection, Use or Disclosure	**Collection of personal information** (POPA sections 2, 4 and 5) The contract specifies that the contractor will collect personal information on behalf of the contractor and specify the authority under POPA for this collection. **Note**: Any collection must be limited to the personal information that is necessary for the service provider to perform the services.		
	The contract specifies what personal information may be collected by the service provider and prohibits the collection of any other personal information.		
	The contract requires the service provider to adhere to the requirements in POPA for collecting personal information, including for direct collection and notice. Any permitted indirect collection is identified in the contract along with the legal authority for this indirect collection.		
	The contract requires the service provider to give notice as required by section 5(2)(d) of POPA if the personal information collected will be entered into an automated system to generate content or make decisions, recommendations or predictions.		
	The contract requires that when collecting personal information from an individual, the service provider or its employees inform the individual that it/they are a service provider to the public body, performing the services on behalf of the public body, that the collection is subject to POPA, and that they are authorized thereunder to collect the information. Note: This could be done by way of notice.		

TOPIC	DESCRIPTION	YES	NO (Reason)
	Accuracy of personal information (POPA section 6) The contract requires that the service provider make every reasonable effort to ensure the accuracy and completeness of any personal information collected where this information will be used to make a decision that will directly affect the individual to whom the information relates. The contract requires that this information be retained for at least one year after using it to make a decision.		
	Use of personal information (POPA sections 11, 12, 14, 17) The contract specifies the permitted uses of the personal information (including any generated, such as derived data) by a service provider and the authority under POPA for this use.		
	The contract requires the service provider to adhere to the requirements in POPA for any use of the personal information including that it may only use this personal information to the extent necessary to enable the service provider to carry out its permitted use.		
	The contract restricts the service provider from using the personal information other than as permitted in the contract. **Note**: consider including a non-exhaustive list of prohibited activities to provide clarity, such as for marketing or training systems to improve services.		
Legal Authorities for Collection, Use or Disclosure	**Disclosure of personal information** (POPA sections 13 and 19) The contract specifies the permitted disclosures of personal information, including what specific personal information may be disclosed, and the authority under POPA for these disclosures. Note: If the service provider is permitted to disclose personal information with consent, then the contract should set out the process for obtaining consent as required by POPA and section 2 of the Regulation.		
	The contract restricts the service provider from disclosing personal information other than as permitted in the contract and the service provider is required to adhere to the requirements in POPA for any permitted disclosures of the personal information.		
	The contract requires the service provider to notify the public body if it receives any request or demand for disclosure of personal information for a purpose not authorized under the contract, and which may be required by law, immediately on receiving the request or demand and must not disclose the personal information unless permitted to do so in writing by the public body.		

TOPIC	DESCRIPTION	YES	NO (Reason)
Requests for Access or Correction	**Access to information and Correction requests** (ATIA section 7) The contract requires the service provider to respond to and manage, on behalf of the public body, access requests received under section 7 of ATIA or and/or correction request under section 7 of POPA. • Roles and responsibilities of each of the public body and service provider are clarified. • The specific responsibilities of the service provider for access request and correction requests are set out in the contract. • The contract specifies reporting requirements concerning responses to access requests. • Interaction with the OIPC for reviews, as between the parties, is specified as to roles and responsibilities concerning this interaction.		
	The contract requires the service provider to cooperate with the public body for any access to information or correction requests received by the public body, including requests made for information, other than just for personal information, that may be subject to the right of access under ATIA.		
Safeguards and Retention	**Protection of personal information** (POPA sections 10, 20, 25(2) and M-Regulation section 7) The contract requires the service provider to implement reasonable security arrangements to protect the personal information, which arrangements must, at minimum, meet the requirements of the public body's administrative, technical and physical safeguards and its security classification system, as set out in its PMP, and in accordance with POPA and section 7 of the M-Regulation. **Note**: The public body must make an assessment of the service provider's security policies and procedures to ensure they meet this threshold if the service provider does not adopt the public body's security policies and procedures for protecting the personal information.		
Safeguards and Retention	**Retention of records or personal information** (POPA sections 6 and 18(1)) The contract specifies the retention and disposal requirements that the service provider must adhere to for records or personal information, including data derived from personal information and non-personal data, including the minimum and maximum retention period and the secure disposal methods to be used. Note: When personal information is used to make a decision about an individual there are specific retention requirements (see Accuracy of personal information).		
	The contract specifies the conditions governing the disposition of any records containing personal information and sets out a certification process.		

TOPIC	DESCRIPTION	YES	NO (Reason)
	The contract specifies retention requirements for audit logs that are long enough for any investigations undertaken by the service provider, public body, and the OIPC concerning the duties of the service provider and their employees or subcontractors under the contract as they relate to the collection, use, disclosure, security and management of the personal information as set out in the contract.		
	Downstream adherence to the contract The contract requires all employees to sign a confidentiality agreement that ensures the service provider's compliance with its duties under the contract and with POPA and ATIA.		
	The contract requires the service provider to bind any subcontractors used in providing the service to the requirements of the service provider in the contract as it relates to the personal information.		
	The contract requires the service provider to train all its employees and any subcontractors who will have access to the personal information on the service providers duties under the contract as it relates to the personal information and for its obligations under POPA. The contract requires retraining to occur on an annual basis. The contact requires the service provider to inform the public body in writing when this training occurs and to whom it was given and when.		
	The contract requires the service provider to provide the public body with a copy of its training material including any updates.		
	Privacy and security assessments (POPA sections 10 and 26, section 1(1)(c) of the Regulation, and sections 2, 3 and 7 of the M-Regulation. The contract requires the service provider to cooperate in the development and any updating of any PIAs required to be created under POPA by the public body and for any required to be submitted to the OIPC for review. The contract requires the service provider to cooperate in a review of a PIA conducted by the OIPC.		
	The contract requires the service provider to conduct a security threat risk assessment at intervals specified in the contract, or as requested by the public body, as a measure to satisfy the public body that the personal information will be reasonably protected.		
Safeguards	**Notification of breach** (POPA section 10(2)) "Breach" is defined in the contract as "an incident involving the loss of, unauthorized access to or unauthorized disclosure of personal information".		

TOPIC	DESCRIPTION	YES	NO (Reason)
	The contract specifies what the service provider is to do if there is a breach (unauthorized access to or disclosure of personal information or loss), including: • the service provider must immediately notify the public body's Privacy Officer on learning about the breach; • the service provider's employees and subcontractors must immediately notify the service provider on learning about a breach; • it must cooperate with the public body on containment and management of the breach; • it must cooperate with the public body on meeting any of its notice requirements to affected individuals, the Minister and the Commissioner about the breach; and it must work with the public body on implementing any measures as may be necessary, or as recommended by the OIPC, to mitigate the risk of recurrence.		
Complaints Handling	**Complaints and investigations** (POPA section 38) The contract addresses how complaints received by the service provider concerning any allegation of non-compliance by the service provider (or its employees or subcontractors) with POPA will be addressed and managed and roles and responsibilities relating thereto are addressed in the contract.		
Termination	**Termination or expiry of the contract** The contract sets out how the contract may terminate including that it may terminate for breach of contract.		
	The contract addresses what is to happen to the records on termination of the contract, including when the contract is terminated for breach of its provisions, such as all personal information and records must be returned to the public body on termination of the contract and that the service provider shall not keep copies of the information.		
	The contract includes clear expectations regarding portability of the records created by the service provider, including those containing personal information, to ensure that on termination, the information can be moved across different platforms with minimal integration issues and it will be readable to the public body.		
	The contract requires that the duty of the service provider to keep confidential the personal information to which it has access during the term of the contract extends beyond the term of the contract and is in perpetuity.		

Appendix 7: Unreasonable Invasion of Privacy Guidelines

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

Step 1: Confirm the personal information

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

Step 2: Not an unreasonable invasion of personal privacy

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

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

Step 3: Presumed unreasonable invasion of personal privacy

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

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

Step 4: Other factors to consider

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

1. These factors would weigh in favour of disclosing personal information:

    a) advances public scrutiny;

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

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

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

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

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

    b) the personal information was supplied in confidence;

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

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

Step 5: Disclosure allowance

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

Appendix 8: Delegation Order

DELEGATION

Privacy and Access to Information Powers, Duties and Functions

Pursuant to section 87 of the *Access to Information Act* and section 55 of the *Protection of Privacy Act,* I hereby delegate my powers, duties and functions as head of the public body to the persons who hold the position of _____, and to the extent, set out in the Schedule A, subject to the following conditions:

1) that the person to whom my powers, duties or functions are delegated are bound in the exercise of those powers, duties or functions by the jurisdictional, legislative and administrative limitations to which I am subject;

2) that the powers, duties or functions delegated to any person may also be exercised by another person who holds the person's position in an acting capacity to which he or she has been duly appointed; and

3) that, notwithstanding the delegation of my powers, duties or functions, I may exercise at any time any of the powers, duties or functions delegated.

This delegation is effective on and from the date shown below and shall remain in effect until revoked.

This delegation may be revoked or amended.

Name and position title of the Head	Signature	Date

Schedule A

Powers, Duties, Functions	***ATIA and POPA references***
1. PROGRAM MANAGEMENT	
a) *Ensuring that privacy, access and security program policies and procedures are developed, maintained, and updated, compliant with legislation;*	POPA ss. 25(1), 15(c), 23(1)(iii) POPA MReg. ss. 6(b)(c)(e)ATIA Reg. s. 3(1)
b) *Developing and completing quality assurance processes for implementation of MD of Spirit River organization privacy and access management;*	POPA Part 4 POPA MReg. ss. 1-7
c) *Providing training and resources so that MD of Spirit River employees, volunteers and contracted personnel are fully knowledgeable of their privacy and access duties, roles, responsibilities and practices in compliance with policy and legislation;*	POPA s. 25 POPA MReg. s. 6(d)
d) *Representing MD of Spirit River in dealings with third parties, the provincial government, and the Office of the Privacy Commissioner of Alberta, as necessary;*	ATIA ss. 49(1), 50(4), 59, 63, 66, 71(3)(5) POPA ss. 28, 29(4), 41(6)(8), 44
2. RIGHT OF ACCESS AND CORRECTION	
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, designating records available without a request, providing access to manuals and guidelines and public interest disclosure and notice;*	ATIA Part 1 (ss. 6-37), ss. 86, 90, 91, 96 ATIA Reg. ss. 6, 8
b) *Responding to request for correction of personal information, including, as necessary, transfer of requests, correcting personal information, annotating personal information, notifying recipients;*	POPA ss. 7-9
3. PRIVACY AND SECURITY	
a) *In consultation with MD of Spirit River employees as necessary, providing advice, interpretation and implementation of applicable legislation regarding personal information, including release / non-release, collection, use and disclosure of personal information, data matching, data derived from personal information and non-personal data.*	POPA s. 4, 5, 5(3)(4), 12, 13(1)(s), 13(1)(cc), 13(1)(ee), 15-23, 54(1)(e) POPA MReg. s. 5 POPA Reg. 1(1)(b), 2 ATIA s. 20, 37
b) *Maintaining the security, protection and accuracy of personal information, data derived from personal information and non-personal data in the custody or control of MD of Spirit River in compliance with legislation and policy;*	POPA ss. 6, 10(1), 20, 24
c) *Directing the response to privacy breaches of personal information at MD of Spirit River and its facilities in line with legislation Privacy Breach Response Policy;*	POPA s. 10(2) POPA MReg. s. 4
d) *Completing Privacy Impact Assessments (PIAs) for MD of Spirit River for project-specific personal information systems and practices;*	POPA s. 26
e) *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.*	POPA s. 57

Appendix 9: Information Security Classification and Standards Table

Class	Harm	Information Type	Security Zones*
Restricted R	• Harm to operations of facilities or security systems • Immediate harm to health and safety of the public, clients, or employees • Loss of source record and accountability	• Information describing security systems, access codes, etc. • Personal or other information that would likely cause or allow a person to harm themselves or specific employees, or clients • Back-up of essential records	Network: Restricted Physical: Restricted
Confidential C	• Humiliation, damage to reputation • Identity theft • Financial or asset loss • Credit loss • Loss of employment, business or professional opportunity Harm to privacy of the public and employees • Economic loss for MD of Spirit River or third parties • Damage to MD of Spirit River credibility or service integrity • Legislative sanctions • Loss of source record and accountability	• All personal and employee information, including highly sensitive personal information • Data derived from personal information • Information given in confidence or under privilege • Third party business information • Deliberations, investigations, advice, decisions • Security audit tools • Non-personal data that has not been assessed and verified.	Network: Internal; External by approval Physical: Internal; External by approval;
Internal Use I	Loss of source record and accountability	• Employee circulars • Administrative records available to public upon request, e.g., completed decisions, policies, reports	Network: Internal or External Physical: Internal or External;

Class	Harm	Information Type	Security Zones*
		• Source records of public information	
Public P	No identified harms	• Published materials such as pamphlets, newsletter, annual reports • Public information such as directories or web sites • Non-personal data in aggregate or statistical form, in a report, summary or other publication, that has been assessed and verified	No restrictions

Appendix 10: Physical Security Zones Requirements Table

SECURITY ZONE	Requirements		
	Authorization	**Barriers to Zone**	**Monitoring**
RESTRICTED Server rooms HR records areas	• Trusted user function-based by Manager of functional area • Unauthorized trusted user case-based by authorized person • No public access	• Area only accessed only from Internal zone • Locked and accessible to authorized persons only with ID • Unauthorized visitors accompanied by authorized persons	Employee or CCTV surveillance All access logged
INTERNAL Admin/technical areas Front desks/reception areas Individual offices	• Trusted user function-based • Unauthorized trusted user by context • Public access case-based by authorized person	• Areas access from External or Public Zones • Locked and restricted to authorized persons with ID • Public visitors accompanied by authorized persons • Sound barriers	Employee surveillance Non-authorized access logged
EXTERNAL Individual offices Off-sites workplaces: (employee cars/ homes)	• Trusted and Public user by context	• Areas accessed from Public or Internal Zones • Locked areas or containers; marked boundaries • Public visitors unaccompanied but without access to information • Low verbal communication	Unlocked areas under employee surveillance
PUBLIC Waiting areas	None	Open but locked off-hours	Employee or CCTV surveillance

- Trusted User: an employee or authenticated third party accessing a MD of Spirit River network, resource, or building in compliance with MD of Spirit River security policy and under agreement.
- Public User: a user not under MD of Spirit River policy or agreement.

Appendix 11: Network Security Zones Requirements Table

SECURITY ZONE	Requirements						
	User	**Connection**	**Firewall Barriers**	**Zone Authentication**	**Encryption**	**Equipment/Devices**	**Monitoring**
RESTRICTED	Restricted	Internal to LAN/dedicated line		2 factor	Strong	Internal	• Editing and access logging • Reviewed daily or by SIEM
INTERNAL	Trusted	Internal to LAN/dedicated line	Internal DMZ	1 factor	None	Internal/External	• Editing and access logging • Reviewed randomly and regularly or by SIEM
EXTERNAL	Trusted	External via internet	External DMZ	2 factor	Strong	Internal/External	• Editing and access logging • Reviewed randomly and regularly or by SIEM
PUBLIC	Public	External	Full Access				None

- Trusted User: an employee or authenticated third party accessing a MD of Spirit River network or resource, in compliance with MD of Spirit River security policy and under agreement.
- Public User: any other user.

Appendix 12: 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

Appendix 13: Privacy Breach Response Form

Privacy Breach Response

Breach #

1. IDENTIFCATION AND REPORTING

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

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

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

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

Reported by:
Name: _____ Position/Role:
Contact information:

Summary of breach as reported

2. CONFIRMATION, CONTAINMENT

Breach Level: Breach location:

Applicable Class and Breach Characteristics:

Potential Harm:

☐ Physical harm to a person
☐ Humiliation or damage to reputation
☐ Financial
☐ ID theft, fraud

*identification of any of the above harms indicates a real risk of significant harm, requiring notification to the individual, the OIPC and the Ministry

Other:

Additional information about breach:

Content and volume of personal information breached:

Recipient name(s) and contact information:

Containment actions and dates:

☐ Contained: _____ / _____ / _____ Time: _____AM/PM
MM / DD / YYYY

☐ Not contained

3. NOTIFICATIONS

Who has been informed of the incident?

☐ Information and Privacy Commissioner informed: _____ / _____ / _____
MM / DD / YYYY

Consultation decision:
Date: _____ / _____ / _____
MM / DD / YYYY

☐ Information and Privacy Commissioner not informed

Notification actions and dates:

☐ Notifications completed: _____ / _____ / _____
MM / DD / YYYY

☐ No notifications or incomplete actions:

4. INVESTIGATION

Investigative actions and dates:

Date	Individuals consulted/investigated and contact information	Role (subject, perpetrator, expert, witness)

Date	Documents/Data Consulted

5. REPORT AND FOLLOW-UP	
Findings:	
Recommendations: Remediation: Prevention:	
Report distribution:	
	_____ / _____ / _____ MM / DD / YYYY
	_____ / _____ / _____ MM / DD / YYYY
	_____ / _____ / _____ MM / DD / YYYY
	_____ / _____ / _____ MM / DD / YYYY
	_____ / _____ / _____ MM / DD / YYYY
Follow up actions planned or executed	
	_____ / _____ / _____ MM / DD / YYYY
	_____ / _____ / _____ MM / DD / YYYY
	_____ / _____ / _____ MM / DD / YYYY
	_____ / _____ / _____ MM / DD / YYYY
6. APPROVALS AND AUTHORIZATIONS	
Name and signature of Investigator _____ Date: _____ / _____ / _____ MM / DD / YYYY	

Name and signature of applicable Leadership

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

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

Appendix 14: Complaint Submission Form

Privacy and Access Complaint Submission Form

PART A – COMPLAINT DESCRIPTION AND SUBMISSION

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

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

Privacy and Access Complaint Submission Form

PART B – MD OF SPIRIT RIVER INTAKE

TO BE FILLED OUT BY THE PRIVACY AND ACCESS OFFICE

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

Appendix 15: Complaint Response Letter

[DATE]

[NAME]
[ADDRESS]

Dear [NAME]:

RE: [FILE NUMBER] [COMPLAINT TITLE]

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

Your request was for the following information:

"[COMPLAINT SUBMITTED]."

- [LIST ANY DOCUMENTS RECEIVED WITH THE COMPLAINT].

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

[FINDINGS AND/OR STATEMENT OF JUSTIFICATION].

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

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

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

Office Hours

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

Phone and Email
Toll-Free: 1-888-878-4044
Edmonton office: (780) 422-6860
Calgary office: (403) 297-2728
Email: generalinfo@oipc.ab.ca

Mailing Addresses
Office of the Information and Privacy Commissioner (Edmonton)
#410, 9925 - 109 Street NW
Edmonton, AB T5K 2J8
Office of the Information and Privacy Commissioner (Calgary)
Suite 2460, 801 6 Avenue SW
Calgary, AB T2P 3W2

Sincerely,

[NAME]

Privacy and Information Officer, MD of Spirit River
[OFFICE ADDRESS]
[PHONE NUMBER]

Appendix 16: Sample Collection Notice

E-mail Notice of Confidentiality:

This message, including any attachments, may contain confidential information intended for a specific individual and purpose. If you are not the intended recipient, please delete this message and do not disclose, copy or distribute it.

Example of collection notice:

Your personal information is being collected by MD of Spirit River for the purpose of administering [program or service being requested] and will be disclosed to and used by the relevant program or service area you have requested. Personal information for this service is being collected pursuant to Section XX of the Protection of Privacy Act of Alberta (POPA). If you have any questions about the collection, use or disclosure of your personal information, please contact [Employee Name], [Employee Title], by mail, phone, or email, at [Mail Address], [Phone Number], or [Email Address].