Index # **Title**

Regional Board Policy

PRIVACY MANAGEMENT PROGRAM POLICY

Category:	**Policy Number:**	**Replaces:**	
Type: ☒ Policy ☐ Procedure	**Authority:** ☒ Board ☒ Administrative	**Approved By:** ☒ Board ☒ CAO ☐ Department Head	
Office of Primary Responsibility: Administration			
Date Adopted:	**Board Resolution Number:**	**Date to be Reviewed:**	
Manner Issued:			

PURPOSE

The purpose of the Cariboo Regional District's Privacy Management Program Policy is to describe how the CRD collects, uses, discloses and protects personal information. This policy provides a framework for how the CRD will operate in order to ensure personal information is managed in accordance with the *Freedom of Information and Protection of Privacy Act (FOIPPA)*.

Implementation of this policy is intended to:

- Set expectations for privacy accountability, and
- Support compliance with the privacy requirements of FOIPPA.

SCOPE

This policy applies to all employees, volunteers, service providers, officers, and directors of the CRD.

This policy applies to personal information that the CRD collects, uses or discloses in any form (including verbal, electronic or written personal information).

*The CRD requires third-party service providers to demonstrate full compliance with the CRD's privacy obligations, principles and processes as outlined in this policy.

DEFINITIONS

Act	means the *Freedom of Information and Protection of Privacy Act* (BC)
Commissioner	means the Information and Privacy Commissioner for BC.
Contact Information	is defined as any information that would enable an individual to be contacted at their place of work.
FOIPPA	means the *Freedom of Information and Protection of Privacy Act.*
Indirect Collection	is defined as the collection of personal information from a source other than the individual for whom the information is about.
Personal Information	is defined as recorded information about an identifiable individual (excluding contact information). Examples of personal information include: name, residential address and telephone number, ethnic origin, sex, marital status, employment history, financial information (including financial history), health care history, etc.
Privacy Breach	means the theft or loss, or the collection, use or disclosure that is not authorized by the *Freedom of Information and Protection of Privacy Act*, of personal information in the custody or under the control of a public body.
Privacy Impact Statement	means a tool used to help assess risks to privacy and protect personal information.
Privacy Officer	means the Deputy Corporate Officer, who is responsible for being a point of contact for privacy-related matters; supporting the development, implementation and maintenance of privacy policies and procedures; and supporting the public body's compliance with FOIPPA.
Public Body	means the Cariboo Regional District.

CRD	means the Cariboo Regional District.
Service Provider	means a person or business retained under a contractual agreement to perform services for the CRD.
Us	refers to the CRD, as do "our," "we," and similar terms, not to any employees or elected or appointed CRD officials.
You	refers to anyone whose personal information we collect, use or disclose.

OBJECTIVE

This policy is designed to comply with Division 4—Privacy Management Programs and Privacy Breach Notifications of Bill 22—2021 *Freedom of Information and Protection of Privacy Amendment Act*, 2021.

POLICY

1. COLLECTION OF PERSONAL INFORMATION

We collect personal information:

a. where collection is authorized under a statute, such as the *Community Charter* (British Columbia) and the *Local Government Act* (British Columbia), or is authorized under CRD bylaws;
b. for the purposes of our activities, services and programs;
c. for the purposes of planning or evaluating our activities, services and programs;
d. for law enforcement purposes, including enforcing our bylaws; and
e. at presentations, ceremonies, performances, sporting events, or similar events, that are open to the public and where you voluntarily appear, such as public meetings and public hearings.

We collect your personal information directly from you, but we may also collect it from another source if you have consented to our doing so. We may also collect your personal information from another source as permitted under the Act, including in these cases:

f. where another law allows us to do so;
g. for law enforcement, for a court proceeding, to collect a debt or fine from you, or to make a payment to you;
h. where your personal information is necessary for us to deliver, or evaluate, a common or integrated program or activity;
i. where your personal information is necessary to establish, manage or terminate an employment relationship between you and us;
j. if your personal information may be disclosed to the CRD under Part 3 of the Act; or

k. where we collect your personal information for the purpose of determining your suitability for an honour or award.

2. USE AND DISCLOSURE OF PERSONAL INFORMATION

We will use and disclose your personal information only for the purpose we collected it for or for a purpose that is consistent with why we collected it in the first place.

We may also use or disclose your personal information for another purpose if you have identified the information and consented to the other use. Lastly, we may use your personal information for a purpose for which it can be disclosed to us under Part 3 of the Act. We may also disclose your personal information:

a. if you have identified the information and consented in writing to its disclosure;
b. to our employees or service providers if the information is necessary for their duties, for delivery of a common or integrated program or activity, or for planning or evaluating a CRD program or activity;
c. if your personal information is made publicly available in British Columbia by a law that authorizes or requires it to be made public;
d. to a public body or law enforcement agency to assist in a specific investigation or law enforcement proceeding;
e. to your union representative who is making an inquiry, if you have given the representative written authority to make the inquiry or it is otherwise authorized;
f. to our legal counsel for the purpose of legal advice or for use in legal proceedings involving us;
g. to your Member of the Legislative Assembly if you have asked them to help resolve a problem; or
h. as otherwise permitted or required under Part 3 of the Act.

Please note that all information provided at open meetings of the Board or its committees is considered to be public. If you provide or disclose your personal information to us for that purpose, you are consenting to that information being available to the public, including through posting on our website or audio or video recording. This information is considered to be a part of the public record and cannot be removed or changed. However, if you satisfy us in advance that you have legitimate personal safety concerns for yourself or an immediate family member, we may allow you to submit your personal information to the Board or a committee in confidence. We will not make it publicly available in that case, although we will keep it in our Corporate Administration office, as part of the record.

3. SAFEGUARDING OF PERSONAL INFORMATION

The CRD administers the highest security standards to ensure the personal information in its custody and/or control is secure at all times. CRD employees and service providers are responsible for ensuring the physical and technical security of all data (including data at rest or in transit) and must meet all applicable security standards.

4. ACCURACY OF PERSONAL INFORMATION

The CRD makes every reasonable effort to ensure that personal information we use to make a decision directly affecting you is accurate and complete.

5. ACCESS TO PERSONAL INFORMATION

You can ask us to give you a copy of your personal information that is in our custody or control by contacting the Corporate Administration department. If you are an employee and would like a copy of your own employee personal information, you will need to contact the Human Resources department. If we believe your request may involve someone else's personal information, or information protected under the Act, we may require you to make a formal request under the Act for access to records. The Act gives us 30 business days to respond to a formal request, starting on the date your request is received (the Act also allows that time to be extended). Please note that in some cases the Act may require us to refuse you access to even your own personal information. We will give you written reasons for every decision on a formal request. Before disclosing your personal information, we will require you to verify your identity, so we can be assured that you are the individual whose information is being requested. This helps ensure we do not disclose your personal information to someone to whom it should not be given.

6. CORRECTION OF PERSONAL INFORMATION

If you believe there is an error or omission in or from your personal information, you can contact the CRD in writing and ask us to correct it. If we decide to correct your information, we will do so as soon as reasonably possible. If we decide not to correct your information, we will note your requested change on the information as well as why we did not correct your information as you asked.

7. RETENTION AND DISPOSAL OF PERSONAL INFORMATION

The CRD and its service providers utilize records retention policies customized for each area. This customization takes into account the length of time information must be retained. If an individual's personal information is used to make a decision, a record of that decision will be kept for a minimum of one year after the decision has been made. Once personal information is no longer needed it is authorized for destruction and confidentially disposed of.

8. USING THE CRD WEBSITE

The CRD website automatically collects and stores the following information from visitors to the website:

- the internet protocol (IP) address and domain name used (the IP address is a numeric identifier assigned to either the individual's internet service provider or directly to the computer)
- the type of browser and operating system
- the date and time of the visit
- the webpage(s) accessed
- amount of time spent on each page

Information automatically collected is used only for the purposes of administering the website, assessing system performance, improving services and website management. The CRD will not use this data to determine the inquirer's identity unless required to do so as part of an internal investigation for law enforcement purposes.

Personal information such as names, email addresses and demographic information is only obtained when individuals supply it voluntarily through contacting us via email or using the forms available on our website. This information will only be used for statistical purposes and to support your relationship with the CRD.

9. LINKS TO OTHER WEBSITES

The CRD website may include links to webpages operated by other organizations. These links are not intended to be referrals and are posted only for convenience. The CRD has no responsibility for, liability, or control over these links or websites. Please refer to the individual privacy policies and terms and conditions of use for external sites.

If you have any questions or concerns regarding the collection, use, disclosure or safeguarding of personal information associated with this website, please contact mailbox@cariboord.ca

10. PROCEDURE – PRIVACY COMPLAINTS AND BREACHES

Any complaint about any privacy-related matter under this policy or under the Act must be made to us in writing. We will consider your complaint, including about a breach of your privacy, and will disclose the outcome to you in writing. We expect you to co-operate reasonably and in a timely way with our work, including by promptly providing us with information that we might reasonably need to do our work. Your failure to do so may result in our deciding not to proceed any further with your complaint. You can make a written formal complaint to the Office of the Information and Privacy Commissioner for British Columbia, although we encourage you to use our complaint procedure first. Wherever we can, we try to work things out directly with people, to their satisfaction.

Requirement to Notify

1. Should a privacy breach occur, the Privacy Officer must be contacted, in writing, without reasonable delay.
2. Then, the Privacy Head, will, without reasonable delay:
    (a) notify an affected individual if the privacy breach could reasonably be expected to result in significant harm to the individual, including identity theft or significant:
    (i) bodily harm,
    (ii) humiliation,
    (iii) damage to reputation or relationships,
    (iv) loss of employment, business or professional opportunities,
    (v) financial loss,

(vi) negative impact on a credit record, or
(vii) damage to, or loss of, property, and

(b) notify the Commissioner if the privacy breach could reasonably be expected to result in significant harm referred to in paragraph (a) above.

How to Notify

Direct Notifications— Affected Individuals

Notifications must include the following information:

- the name of the public body;
- the date on which the privacy breach came to the attention of the public body;
- a description of the privacy breach including, if known,
    a) the date on which or the period during which the privacy breach occurred, and
    b) a description of the nature of the personal information involved in the privacy breach;
- confirmation that the Commissioner has been or will be notified of the privacy breach;
- contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;
- a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

Indirect Notifications—Affected Individuals

A notification may be given to an affected individual in an indirect manner if:

a) the public body does not have accurate contact information for the affected individual,

b) the head of the public body reasonably believes that providing the notice directly to the affected individual would unreasonably interfere with the operations of the public body, or

c) the head of the public body reasonably believes that the information in the notification will come to the attention of the affected individual more quickly if it is given in an indirect manner.

If a notification must be given in an indirect manner, the notification must

a) be given by public communication that can reasonably be expected to reach the affected individual, and
b) contain the following information:
    - the name of the public body;
    - the date on which the privacy breach came to the attention of the public body;
    - a description of the privacy breach including, if known,
        a) the date on which or the period during which the privacy breach occurred, and
        b) a description of the nature of the personal information involved in the privacy breach;
    - confirmation that the Commissioner has been or will be notified of the privacy breach;
    - contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
    - a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individual;
    - a description of steps, if any, that the affected individual could take to reduce the risk of harm that could result from the privacy breach.

Notifications – Commissioner

A notification under section 36.3 (2)(b) of the Act must be given to the Commissioner in writing and must include the following information:

- the name of the public body;
- the date on which the privacy breach came to the attention of the public body;
- a description of the privacy breach including, if known,
    a) the date on which or the period during which the privacy breach occurred,
    b) a description of the nature of the personal information involved in the privacy breach, and
    c) an estimate of the number of affected individuals;
- contact information for a person who can answer, on behalf of the public body, questions about the privacy breach;
- a description of steps, if any, that the public body has taken or will take to reduce the risk of harm to the affected individuals.

Not Required to Notify

1. The head of a public body is not required to notify an affected individual under section 36.3(2) of the Act if notification could reasonably be expected to

    (a) result in immediate and grave harm to the individual's safety or physical or mental health, or
    (b) threaten another individual's safety or physical or mental health.

11. PRIVACY IMPACT ASSESSMENTS

Privacy Impact Assessments (PIAs) are conducted to determine if a proposed system, project, program or activity meets or will meet the requirements of Part 3 of FOIPPA. A PIA will be done for any new system, project, program or activity involving personal information and for any new collection, use or disclosure of personal information. A PIA will also be conducted for common or integrated programs or activities and data-linking initiatives, as well as when significant modifications are made to existing systems, projects, programs or activities.

Employees initiating new systems, projects, programs or activities that involve collecting, using, storing or sharing personal information are required to complete a PIA (Schedule A attached) and submit it to the Privacy Officer.

12. SERVICE PROVIDER MANAGEMENT

Employees who prepare or manage contracts with service providers are to include the privacy protection schedule or standard privacy language, as designated by the Privacy Officer, in all contracts that involve the service provider having access to, or collecting, using or disclosing, personal information in the custody or under the control of the CRD.

13. INFORMATION SHARING AGREEMENTS

If initiatives include a regular or systematic exchange of personal information with partners outside of the public body, an Information Sharing Agreement must be completed (Schedule B attached) and submitted to the Privacy Officer.

14. EDUCATION AND AWARENESS

All CRD employees receive training on the Act and privacy generally as appropriate to their work function. Additional training is given in the following circumstances:

- Employees handling what we consider high-risk or sensitive personal information electronically receive training related to information systems and their security, in coordination with the IT department;
- Employees managing programs or activities receive training related to privacy impact assessments; and
- Employees managing common or integrated programs or activities receive training related to information sharing agreements.

15. ROLES AND RESPONSIBILITIES

Board of Directors:

- Approves policy and procedures.

Department Heads:

- Support and cooperate with the Privacy Officer in implementing the policy and in complying with FOIPPA.

Manager of Corporate Services/Deputy Corporate Officer:

- Responsible for the development, management and implementation of the CRD's privacy management program including ongoing assessments and revisions.
- Coordinates employee training and education, ensuring that all new employees receive FOIPPA orientation and training within the first year of their employment.

16. AUTHORITY TO ACT

The Manager of Corporate Services is delegated responsibility and authority for ensuring compliance with this policy and FOIPPA.

17. RELATED DOCUMENTS

- *Freedom of Information and Protection of Privacy Act* [RSBC 1996] Chapter 165
- Cariboo Regional District Freedom of Information and Protection of Privacy Bylaw No. 5261, 2020

18. REVIEW

This policy shall be reviewed by the Manager of Corporate Services at least every 3 years.

19. ACCESS TO PERSONAL INFORMATION AND QUESTIONS REGARDING PRIVACY

Inquiries, complaints, or access requests should be addressed to:

Deputy Corporate Officer/Privacy Officer, CRD
250.392-3351 | **mailbox@cariboord.ca**

For more information, please visit: the Office of the Information and Privacy Commissioner.

The CRD may change this policy when it is appropriate to do so. As such, it is recommended users review the policy regularly.

Schedule A: Privacy Impact Assessment

Table of Contents

Use this Privacy Impact Assessment (PIA) template if you work for, or are a service provider to the Cariboo Regional District (CRD) and are starting a new initiative or significantly changing an existing initiative.

Before you start

- An initiative is an enactment, system, project, program or activity
- If you have any questions, email mailbox@cariboord.ca or call 250.392-3351.

PART 1: GENERAL INFORMATION

Initiative title:	
Organization:	

Department:	
Your name and title:	
Your work phone:	
Your email:	
Initiative Lead name and title:	
Initiative Lead phone:	
Initiative Lead email:	
Privacy Officer:	
Privacy Officer phone:	250.392.3351
Privacy Officer email:	mailbox@cariboord.ca

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
Related PIAs, if any:

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you are doing, how it works, who is involved and when or how long your initiative runs.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

3. What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix.

3.1 **Did you list personal information in question 3?**

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Type "yes" or "no" to indicate your response.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

4. How will you reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 1:			
Step 2:			
Step 3:			
Step 4:			

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

6. Collection Notice

If you are collecting personal information directly from an individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

Review the sample collection notice and write your collection notice below. You can also attach the notice as an appendix.

PART 3: STORING PERSONAL INFORMATION

If you are storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

Type “yes” or “no” to indicate your response.

8. Where are you storing the personal information involved in your initiative?

9. Does your initiative involve sensitive personal information?

Type "yes" or "no" to indicate your response.

- If yes, go to question 10
- If no, go to Part 5

10. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

Type "yes" or "no" to indicate your response.

- If yes, go to Part 5
- If no, go to Part 4

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer. More help is available in the Guidance on Disclosures Outside of Canada.

11. Is the sensitive personal information stored by a service provider?

Type "yes" or "no" to indicate your response.

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

13. Does the contract you rely on include privacy-related terms?

Type “yes” or “no” to indicate your response.

- If yes, describe the contractual measures related to your initiative.

15. What controls are in place to prevent unauthorized access to sensitive personal information?

16. Provide details about how you will track access to sensitive personal information.

17. Describe the privacy risks for disclosure outside of Canada.

Use the table to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk you identify describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	**Impact to individuals**	**Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)**	**Level of privacy risk (low, medium, high, considering the impact and likelihood)**	**Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)**	**Is there any outstanding risk? If yes, please describe.**

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the Privacy Officer of the CRD on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The CRD may document the decision in an appropriate format as determined by the Head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations or governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

18. Does your initiative involve digital tools, databases or information systems?

Type "yes" or "no" to indicate your response.

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

18.1 **Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?**

Type "yes" or "no" to indicate your response.

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

19. What technical and physical security do you have in place to protect personal information?

Describe where the digital records for your initiative are stored (e.g., on your organization's local area network, on your computer desktop, etc.) and the technical security measures in place to protect those records. Technical security measures include secure passwords,

encryption, firewalls, etc. Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.

If you have completed a security assessment, you may want to append it to the PIA.

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information	
Employees that need standing or recurring access to personal information must be approved by department manager	
We use audit logs to see who accesses a file and when	
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

22.1 **Do you have a process in place to correct personal information?**

Type "yes" or "no" to indicate your response.

22.2 **Sometimes it is not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you are not able to correct the record itself. Will you document the request to correct or annotate the record?**

Type "yes" or "no" to indicate your response.

22.3 **If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third party of the request for correction. Will you ensure that you conduct these notifications when necessary?**

Type "yes" or "no" to indicate your response.

23. Does your initiative use personal information to make decisions that directly affect an individual?

Type "yes" or "no" to indicate your response.

- If yes, go to question 24
- If no, skip ahead to Part 7

24. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision.

Type "yes" or "no" to indicate your response.

- **If no, describe how you will ensure the information will be kept for a minimum of one year after it is used to make a decision that directly affects an individual.**

PART 7: PERSONAL INFORMATION BANKS

A Personal Information Bank (PIB) is a collection of personal information searchable by name or unique identifier.

25. Will your initiative result in a Personal Information Bank?

Type "yes" or "no" to indicate your response.

- If yes, please complete the table below.

Describe the type of information in the bank
Name of main organization involved
Any other ministries, agencies, public bodies or organizations involved
Business contact title and phone number for person responsible for managing the Personal Information Bank

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

26. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Add new rows if necessary.

Possible risk	**Response**
Risk 1:	
Risk 2:	
Risk 3:	
Risk 4:	

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Officer Comments

Privacy Officer Signatures

This PIA is based on a review of the material provided to the Privacy Officer as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Officer Representative			

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored or disclosed, the program area will engage with the Privacy Officer and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead			
Program/Department Manager			
Contact Responsible for Systems Maintenance and/or Security Only required if they have been involved in the PIA			
Head of public body, or designate (if required)			

Schedule B—Information Sharing Agreement

If your initiative includes or will be part of a regular and systematic exchange of personal information with partners in or outside of the CRD, you may require an Information Sharing Agreement (ISA).

Please provide information about your ISA and once complete, submit to the Privacy Officer.

Description of ISA
Name of CRD department involved:
Any other ministries, agencies, public bodies or organizations involved:
Business contact title and phone number for person responsible for maintaining the ISA:
ISA start date:
ISA end date:

***** END OF POLICY *****

Amended (Y/N)	Date Reissued	Authority (Resolution #)