|  |  |
| --- | --- |
| **Public Body Name:** |  |
| **Name of Project:** |  |
| **Expected Go-Live Date:** |  |

|  |
| --- |
| **PIA Team** |
| **Name** | **Position** | **Division/Department** | **Phone #** | **Email** |
| (Lead) |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Executive Summary

### This is a descriptive summary of the project.

### See p. 9 in the PIA Guide for additional details.

# Project Summary

# (Refer to Section 1of the PIA Guide)

Provide a full description of the proposed project, or what is changing with an existing project, including its objectives. State why the system must collect, use or disclose personal.

**Project Description**

|  |  |
| --- | --- |
| **Purpose of Project:** |  |
| **Scope of Project:** | *Is this project a new project or an upgrade or modification of existing project?* |  |
| **Previous PPIA/PIA:** | *Was a PPIA or PIA completed previously for this project?* |  |
| **Benefits of the Project:** |  |

# Information Flow Analysis

(Refer to Section 2 of the PIA Guide)

Complete the table below for each type of personal information being collected (e.g. name, address, etc.)

*Please note that #1 is completed as an example. Please remove before completing this table.*

**Personal Information Table:**

| **#** | **Personal Information** | **Purpose** | **Collected By** | **Used by** | **Disclosed to (if applicable)** | **Information Source** |
| --- | --- | --- | --- | --- | --- | --- |
|  | *First and last name* | *Identify and provide service to client* | *Client services managers* | *Employees in Client services division* | *Federal department A* | *Client application form* |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Information Flow Diagram:**

1. Insert the information flow diagram which showshow personal information for the project will be collected, used and/or disclosed.
2. Provide a brief description of the flow of information found in the flow diagram:

# Collection of Personal Information

(Refer to Section 3 of the PIA Guide)

**A. Type and Extent of Personal Information Collected**

3.1 The personal information and accompanying details listed in the personal information table in section 2.0 of this PIA are accurate and complete.

[ ]  Yes

[ ]  No – please explain

**B. Authority for Collection**

List each type of personal information being collected (see personal information table in section 2.0) and list the reason and authority for the collection. *Please note that #1 is completed as an example. Please remove before completing this table.*

**Authority for Collection Table:**

| **#** | **Personal Information** | **Purpose** | **Legislative Authority**  |
| --- | --- | --- | --- |
|  | *First and last name* | *To identify and provide service to clients* | *s.61(c), ATIPPA, 2015* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

3.2 Does this project include data matching between your public body and another entity (e.g. public body, third party, etc.)?

[ ]  Yes –provide additional detail

[ ]  No

**C. Manner of Collection**

*Please note that #1 is completed as an example. Please remove before completing this table.*

**Manner of Collection Table:**

| **#** | **Personal Information** | **Manner of Collection** | **Legislative Authority** |
| --- | --- | --- | --- |
|  | *First and last name*  | *Directly from individual via application form.* | *62(1)(c)(i) ATIPPA* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**D. Privacy Notices**

Complete the following table for any forms being used for this project to collect personal information (either electronic or paper). In addition, attach a copy of each form to this PIA. *Please note that #1 is completed as an example. Please remove before completing this table.*

**Privacy Notices Table:**

| **#** | **Form Name** | **Information Collected** | **Privacy Notice Included** |
| --- | --- | --- | --- |
|  | *Application for subsidy A* | *First and last name, annual income* | *Under the authority of sections 61(c) and 68(1)(c) of the Access to Information and Protection of Privacy Act, 2015, the personal information on this form will be collected and disclosed for the purpose of determining eligibility for the Subsidy A Program and administrative purposes. If you have any questions regarding this collection or disclosure please contact (709) 729-5555.* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**E. Collection Accuracy**

3.3 Is the identity of the applicant verified during collection?

[ ]  Yes

[ ]  No – provide additional detail

3.4 Does the individual confirm that information is complete and correct?

[ ]  Yes

[ ]  No - provide additional detail

**F. Collection Risk Analysis**

Please list potential risks associated with the collection of the personal information for this project, as well as what risk mitigation strategies your public body has implemented to reduce these risks. For a project with an electronic component and where mitigation measures are system-based, the IT representative on your PIA team may need to assist in completing this section. *Please note that #1 is completed as an example. Please remove before completing this table.*

|  |
| --- |
| **Risk Analysis- Collection** |
| **#** | **Potential Risks With Collection**  | **Implemented Risk Mitigation Strategy**  |
|  |  *That all public body employees would have access to sensitive client information* | *Access controls have been added to the database to limit employees with access to only those who require access for their job.* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Use of Personal Information

(Refer to Section 4 of the PIA Guide)

**A. Use**

4.1 Will the public body that collected the information be the primary user of the information?

[ ]  Yes

[ ]  No – list the organization/s that will be using the personal information

Please complete the following table for all personal information used for this project (refer to personal information table in section 2.0) *Please note that #1 is completed as an example. Please remove before completing this table.*

**Personal Information Use Table:**

| **#** | **Personal Information** | **Used By** | **Used For Purpose Of** | **Legislative Authority** |
| --- | --- | --- | --- | --- |
|  | *First and last name* | *Employees in Client services division* | *To determine client eligibility for service A* | *s.66(1)(a), ATIPPA, 2015* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**B. Additional Use**

4. 2 Will the information be used for any additional purposes?

[ ]  Yes – *if yes, complete table below*

[ ]  No

If you answered yes to 4.2, please complete the following table for all personal information collected that is being used for a new purpose. *Please note that #1 is completed as an example. Please remove before completing this table.*

**Additional Use Table:**

| **#** | **Personal Information** | **Original Purpose** | **New Purpose** | **Legislative Authorization** |
| --- | --- | --- | --- | --- |
|  | *Annual income* | *To determine client eligibility for service A* | *To determine client eligibility for service B which offers similar services to service A* | *s.69, ATIPPA, 2015* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**C. Use Risk Analysis**

Please list potential risks associated with the use of the personal information for this project, as well as what risk mitigation strategies your public body has implemented to reduce these risks. *Please note that #1 is completed as an example. Please remove before completing this table.*

|  |
| --- |
| **Risk Analysis - Use** |
| **#** | **Potential Risks With Use**  | **Implemented Risk Mitigation Strategy**  |
|  |  *That all public body employees could use it for additional purposes not authorized under ATIPPA, 2015.* | *Procedures have been updated to clarify when employees can use personal information and training has been provided to all employees regarding the changes to procedures.* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Disclosure of Personal Information

(Refer to Section 5 of the PIA Guide)

*Note, this section covers only regular disclosure as part of program process and does not include unsolicited requests from external public bodies.*

### Disclosure

5. 1 Records will be disclosed outside of the public body?

 [ ]  Yes

[ ]  No – *if no, please proceed to section 6*

5. 2 Records will be disclosed to a third party other than a public body that falls under *ATIPPA, 2015*?

[ ]  Yes - if yes, attach privacy provisions of contract/agreement with service provider.

[ ]  No

If you answered yes to either 5.1 or 5.2, please complete the following table. *Please note that #1 is completed as an example. Please remove before completing this table.*

**Disclosure Table:**

| **#** | **Personal Information** | **Disclosed to** | **Purpose of Disclosure** | **Legislative Authority**  | **Can Purpose Be Achieved Without Disclosure?** |
| --- | --- | --- | --- | --- | --- |
|  | *First and last name, annual income* | *Federal Department A* | *To determine eligibility for service* | *68(1)(b), ATIPPA, 2015* | *No* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**B. When Disclosure is with Consent**

If you listed the authority for disclosure in the table above as section 68(1)(b) of *ATIPPA, 2015* this means that you will receive individuals’ consent to disclosure their personal information.

If consent is collected on a form other than the form where other personal information is collected, attach the consent form or copy the wording of the consent to this PIA.

For those instances where you will receive consent for disclosure, check each item under “Consent Criteria” that apply:

|  | **Consent Criteria** | **Criteria Met? Yes/No** |
| --- | --- | --- |
| **🞎** | The purpose for disclosure is clear and concise |  |
| **🞎** | The person giving consent is authorized to give consent |  |
| **🞎** | Consent is voluntary |  |
| **🞎** | Consent is in writing or annotated |  |
| **🞎** | An explanation of the impact of consent or not providing consent is provided |  |
| **🞎** | Individual is able to withdrawn consent |  |

**C. Disclosure Risk Analysis**

Please list potential risks associated with the disclosure of the personal information for this project, as well as what risk mitigation strategies your public body has implemented to reduce these risks. *Please note that #1 is completed as an example. Please remove before completing this table.*

|  |
| --- |
| **Risk Analysis - Disclosure** |
| **#** | **Potential Risks With Disclosure** | **Implemented Risk Mitigation Strategy**  |
|  |  *The third party does not fall under ATIPPA, 2015 and is not required to follow its privacy provisions* | *A privacy clause has been added to the contract with the third party requiring it to follow the privacy provisions of ATIPPA, 2015 in regards to the personal information disclosed.* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Safeguards and Security

(Refer to Section 6 of the PIA Guide)

Section 64 of *ATIPPA, 2015* requires a public body to protect personal information in its custody or control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

**A. Physical Safeguards**

| **#** | **Safeguard** | **Yes/No** | **Further Details**  |
| --- | --- | --- | --- |
|  | Locked Filing Cabinets |  |  |
|  | Secure Storage Areas |  |  |
|  | Secure Building Access |  |  |
|  | Security Systems |  |  |
|  | Other |  |  |

**B. Administrative Safeguards**

| **#** | **Safeguard** | **Yes/No** | **Further Details** |
| --- | --- | --- | --- |
|  | Security Clearances/Background Checks |  |  |
|  | Privacy Clauses in 3rd Party Contracts |  |  |
|  | Privacy Policies |  |  |
|  | Account Management |  |  |
|  | Change Management |  |  |
|  | User Warnings |  |  |
|  | Other |  |  |

**C. Technical Safeguards**

For a project with an electronic component, the IT representative on your PIA team may need to assist in completing this section.

| **#** | **Safeguard** | **Yes/No** | **Further Details** |
| --- | --- | --- | --- |
|  | Encryption  |  |  |
|  | Secure disposal of electronic records |  |  |
|  | Auditing capability  |  |  |
|  | Other |  |  |

**D. Access Control**

For a project with an electronic component, the IT representative on your PIA team may need to assist in completing this section.

| **#** | **Access Control** | **Yes/No** | **Further Details** |
| --- | --- | --- | --- |
|  | User authentication |  |  |
|  | Passwords |  |  |
|  | Locking workstations |  |  |
|  | User classifications (e.g. limiting users) |  |  |
|  | Exit procedures |  |  |
|  | Other |  |  |

**E. Positions with Access**

Please list the positions in your public body that will have access to the personal information collected for this project and the functions assigned to each. *Please note that #1 is completed as an example. Please remove before completing this table.*

**Positions with Access Table:**

|  |  |  |
| --- | --- | --- |
| **#** | **Position** | **Functionality Assigned to User** |
| **Read/View** | **Add Content** | **Delete** | **Modify** |
|  | *Client Services Technicians (5)* | *Yes* | *Yes* | *No*  | *Yes* |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**F. Preliminary Threat Risk Assessment**

6.1 Has a Preliminary Threat Risk Assessment been completed by the OCIO?

[ ]  Yes – *if yes, attach completed document or summary to the end of this PIA*

[ ]  No, but one will be completed by *[insert date]*

[ ]  No, one will not be completed – provide explanation

**G. Threat Risk Assessment**

6.2 Has a Threat Risk Assessment been completed?

 [ ]  Yes – *if yes attach completed document or summary to the end of this PIA*

[ ]  No, but one will be completed by *[insert date]*

[ ]  No, one will not be completed – provide explanation

**H. Vulnerability Assessment**

6.3 Has a Vulnerability Assessment been completed?

 [ ]  Yes – *if yes attach summary to the end of this PIA*

[ ]  No, but one will be completed by *[insert date]*

[ ]  No, one will not be completed – provide explanation

**I. Other Assessment**

6.4 Have any other security and/or information risk assessments been completed (e.g. security design review, etc.)?

 [ ]  Yes – *if yes attach summary to the end of this PIA*

[ ]  No, but one will be completed by *[insert date]*

[ ]  No

**J. Review of Security Safeguards**

|  |  |
| --- | --- |
| A review of Security Safeguards will be conducted every (if applicable): |  |

**K. Risk Analysis**

Please list potential risks associated with the security safeguards for this project, as well as what risk mitigation strategies your public body has implemented to reduce these risks. *Please note that #1 is completed as an example. Please remove before completing this table.*

|  |
| --- |
| **Risk Analysis - Security Safeguards** |
| **#** | **Potential Risks with Security Safeguards** | **Implemented Risk Mitigation Strategy**  |
|  | *The database being used does not have an audit function.* | *Employees with access to the database are limited to those who require it. In addition, these employees will complete privacy training.* |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Privacy Breach Reporting and Management

(Refer to Section 7 of the PIA Guide)

**A. Policies and Procedures**

7.1 Is there an organizational policy and applicable procedures for reporting and managing breaches?

 [ ]  Yes – *if yes, attach policy and procedures to the end of this PIA*

[ ]  In progress

[ ]  No

**B. Previous Privacy Breaches**

List all breaches that have occurred in the Department over the past 2 years.

**Previous Privacy Breaches Table:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Description** | **# of people affected** | **Reported to ATIPP Office** | **Reported to OIPC** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**C. Privacy Breach Risk Analysis**

Please list potential risks associated with privacy breaches for this project, as well as what risk mitigation strategies your public body has implemented to reduce these risks. This section is intended to highlight privacy risks. For IT system security risks, that information would be contained within the corresponding risk assessment completed by the OCIO and referenced above in Section 6. *Please note that #1-3 are completed as an example. Please remove before completing this table.*

|  |
| --- |
| **Risk Analysis- Privacy Breaches** |
| **#** | **Potential Risks of Privacy Breach** | **Implemented Risk Mitigation Strategy**  |
|  | *Employees could access personal information and use or disclose it for personal purposes* | *Oath of Employment* |
|  | *Request may not actually be from client (i.e. their email address may be being used by someone else)* | *Implementation of identification verification procedures*  |
|  | *Inherent risks in sending personal information to a client via email* | *Policy developed to inform clients of risk and ask if they would like the information via a different medium, such as through the mail* |
|  |  |  |
|  |  |  |

# Recommendations

(to be completed by the ATIPP Office)

|  |
| --- |
| **Recommendations**  |
| **Project Status** |
|   | Approved |
|   | Conditionally Approved - subject to recommendations |
|   | Not Recommended  |
|  |  |
| **Risk Analysis** |
| **Potential Risk** | **Overall Risk** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |
| 4 |  |  |
| 5 |  |  |
| **Recommendations** |
| 1 |   |
| 2 |   |
| 3 |   |
| 4 |   |
| 5 |   |
| 6 |   |
| **Follow-up on Recommendations** |
|   | 1 month |
|   | 6 month |
|   | 12 months |

This section is to be completed by the ATIPP Office.

# Final Sign-Off

**Reviewer Signatures**

Before the PIA is finalized, it must be reviewed by the ATIPP Coordinator for the department/public body, the IT representative with OCIO on the PIA team (if projects have an electronic component), and the IM Director with the department/public body.

|  |  |  |
| --- | --- | --- |
| ATIPP Coordinator [Department/Public Body] |  | Date |
| IT Representative, OCIO **(if projects have an electronic component)**  |  | Date |
| IM Director [Department/Public Body] |  | Date |

**Approval Signatures**

Before the PIA is finalized it must be reviewed, approved and signed by the PIA Team Lead, the program manager (if different than the Team Lead), ATIPP Office and Deputy Minister/Equivalent of the public body.

|  |  |  |
| --- | --- | --- |
| PIA Team Lead |  | Date |
| Program Manager **(if not Team Lead)** [Department/Public Body]  |  | Date |
| Senior Privacy Analyst, ATIPP Office |  | Date |
| Deputy Minister/Equivalent, [Department/Public Body]  |  | Date |