Privacy Impact Assessment (PIA) Questionnaire

Assess the protection of privacy Part 2 of the *Freedom of Information and Protection of Privacy Act* (FOIP Act)

Part One: Basic information

1.1 Provide Program Area Identifiers.

Public Body	
Division (if applicable)	
Branch/Unit	
PIA Title	
PIA File Number	

1.2 Provide Program Area Contact Information.

This should be the name of the individual able to respond to questions regarding the PIA or the contact information of the position able to respond in future.

Name/Title	
Branch/Unit	
Telephone	
E-Mail	

1.3 Description of the Initiative/Program/Application/System ("Initiative") under assessment:

Briefly describe what is being done. If this is a change to an existing Initiative, explain what is currently in place and what is proposed to be changed.

*This should include the **scope** of this assessment. For phased projects, define the scope in terms of the phase and have a different PIA for subsequent phases.*

1.4 Purpose/Objective of the Initiative:

Briefly describe the goal of the Initiative or the problem it seeks to overcome. If the purpose is statutory, provide citation. If there is an existing PIA for an earlier version of the initiative, or for a related initiative, you can refer to it.

Any attachment to the PIA should be included as Appendices. Please include a List of Appendices.

1.5 Does the Initiative collect, use or disclose personal information as defined in section 1(n) of the FOIP Act[1]?
For example, are you implementing a collection of personal information that was not previously done? Are you changing the way you collect personal information in an existing Initiative in any way? Are you expanding the scope of the Initiative so more people may be affected? Are other agencies participating in the exchange of personal information under this Initiative? These are the types of questions to consider.

Yes/No

If the answer is YES, or if you are uncertain, continue this assessment.
If the answer is NO, there is nothing further required; go to *Signatures* under Part 12 of this assessment.

1.6 List of personal information data elements being collected, used or disclosed under this Initiative.

For example: Name, telephone number, gender, other personal identifiers, etc. The list of data elements can be provided as an attachment.

*It is important to identify every piece of personal information: i.e. any **"recorded information about an identifiable individual"**.*

1.7 Has any previous personal information privacy or security assessment been done for this Initiative or a related initiative?

Please list for cross-reference any related PIAs, Security Threat and Risk Assessments (STRAs) or other assessments previously completed or concurrently being undertaken.

Remember to include any attachments referenced in the PIA as Appendices.

1.8 Provide a flowchart illustrating the information flows, i.e. the collection, storage movement, use and disclosure of all personal information.

This can be a block and arrow diagram. Make it as simple and as clear as possible.

The purpose of the flowchart is simply to identify where, how and to whom personal information is moving under this Initiative in order to aid identification of legislative authorities at each point of exchange.

Please include below or as an attachment.

Part Two: Collection (section 33)

Is this Initiative collecting personal information? **Yes/No**

If the answer is YES, continue under this part of the assessment.
If the answer is No, go to *Use* under Part 5 of this assessment.

There are three authorities for a public body to collect personal information under the FOIP Act. Please think about all personal information data elements collected. The collection of some personal information data elements may have a different authority than other personal

[1] Under section 1(n) of the FOIP Act, personal information is defined as "recorded information about an identifiable individual" and examples are listed.

information data elements and we must identify every authority that applies. Check all that apply.

☐ The collection of the personal information is expressly authorized by an enactment of Alberta or Canada. [s. 33(a)] *If yes, provide the legislative authority: [Name and section of Act]*

☐ The collection of the personal information is for law enforcement. [s. 33(b)]

Note: law enforcement is defined under section 1(h) of the FOIP Act. In order to apply this authority, please review this definition and Bulletin No. 7: Law Enforcement found at: http://www.servicealberta.gov.ab.ca/foip/resources/bulletins.cfm

☐ The collection of the personal information is directly related to and necessary for an operating program or activity of the public body. [s. 33(c)]

*If yes, explain how the personal information is **both** directly related to and necessary for an operating program or activity of the public body under this Initiative.*

If you have checked any of these three authorities above for collection, you have identified an authority under the FOIP Act that allows the Initiative to collect the personal information. Please continue the assessment.
If the answer is NO to all three of these authorities above, you have not identified an authority under the FOIP Act that allows the Initiative to collect the personal information. Is the Initiative collecting personal information? **Please contact your FOIP Office for assistance.**

.

Part Three: Direct/Indirect collection (section 34)

Personal information must be collected directly from the individual unless an exception to this requirement applies.

Is the Initiative only collecting personal information directly from the individual the information is about? **Yes/No**

If the answer is YES, go to *Notification* under Part 4 of this assessment.
If the answer is NO and you are planning to collect any personal information indirectly, continue under this part of the assessment.

Please indicate whether any of the following statements are true. Please ensure indirect personal information flows are indicated on the preceding flowchart and be prepared to provide additional supporting information. Check all that apply.

☐ The individual authorized (consented to) another method of collection. [s. 34(1)(a)(i)] *If yes, please explain how authorization is obtained:*

☐ Another Act or regulation authorizes the indirect collection. [s. 34(1)(a)(ii)] *If yes, provide the legislative authority: [Name and section of Act]*

☐ The Information and Privacy Commissioner has authorized the indirect collection. [s. 34(1)(a)(iii) with s. 53(1)(h)] *If yes, please provide any details in relation to the Commissioner's authorization such as expiry, conditions, etc:*

☐ The information is disclosed to the public body under the FOIP Act. [s. 34(1)(b)] *If yes, please provide the section of FOIP Act under which the personal information is disclosed to the public body:*

☐ The information is collected in a health or safety emergency and direct collection is not possible or is unsafe. [s. 34(1)(c)]

☐ The collection is from a designated emergency contact or contact for other specified circumstances. [s. 34(1)(d)]

☐ The indirect collection is for the purpose of determining suitability for an honour or award. [s. 34(1)(e)]

☐ The collection is from published or public sources for the purpose of fund raising. [s. 34(1)(f)]

☐ The indirect collection is for the purpose of law enforcement. [s. 34(1)(g)]

Note: law enforcement is defined under section 1(h) of the FOIP Act. In order to apply this authority, please review this definition and Bulletin No. 7: Law Enforcement found at: *http://www.servicealberta.gov.ab.ca/foip/resources/bulletins.cfm*

☐ The indirect collection is for the purpose of collecting a debt or fine owed to the Government of Alberta (GoA) or to a public body. [s. 34(1)(h)]

☐ The indirect collection concerns the history, release or supervision of an individual under the control or supervision of a correctional authority. [s. 34(1)(i)]

☐ The indirect collection is for use in the provision of legal services to the Government of Alberta or a public body. [s. 34(1)(j)]

☐ The indirect collection is necessary to determine eligibility for participation in a program or to receive a benefit, product or service from the GoA/public body and occurs in the course or processing an application. [s. 34(1)(k)(i)]

☐ The indirect collection is necessary to verify eligibility for participation in a program or current receipt of a benefit, product or service from the GoA/public body and the information was collected for that purpose. [s. 34(1)(k)(ii)]

☐ The indirect collection is for the purpose of informing the Public Trustee or a Public Guardian about clients or potential clients. [s. 34(1)(l)]

☐ The indirect collection is for the purpose of enforcing a maintenance order under the *Maintenance Enforcement Act*. [s. 34(1)(m)]

☐ The indirect collection is for the purpose of managing or administering personnel of the GoA/public body. [s. 34(1)(n)]

☐ The indirect collection is for the purpose of assisting in researching or validating the claims, disputes or grievances of aboriginal people. [s. 34(1)(o)]

If you have checked one of the preceding authorities for indirect collection, you have identified an authority under the FOIP Act to collect the personal information from another source rather than directly from the individual(s) themselves. **Notification is not required: skip to *Use* under Part 5 of this assessment.**
If none of these indirect collection authorities is selected, you must collect the personal information directly from the individual the information is about or identify options that meet one or more of these authorities. **Please contact your FOIP Office for assistance.**

Part Four: Notification (section 34)

*Notification is required when personal information is collected directly from an individual. This part of the assessment is completed when you are collecting information directly from individuals. Notification contains **three** elements:*

i) Purpose of collection – This must be specific enough so a reasonable person can understand the purpose for which their personal information is collected including how it may be used and/or disclosed.

ii) Specific legal authority for collection – This should include any enabling legislation and/or the applicable FOIP Act authority.

iii) Job Title, business address and business telephone number of an officer or employee of the public body who can answer questions about the collection.

Does the notification provided to the individual at the time personal information is collected under this Initiative include the three elements listed above? [s. 34(2)] **Yes/No**

Briefly describe how notification for the direct collection of personal information is provided under this Initiative:

(Note: If the head of the public body feels direct collection would result in the collection of inaccurate information [s. 34(3)], contact the FOIP Office.)

Part Five: Use (section 39)

Is the Initiative using personal information? **Yes/No**

If the answer is YES, continue under this part of the assessment.
If the answer is No, go to *Disclosure* beginning at Part 6 of this assessment.

There are three use authorities for personal information under the FOIP Act. Please think about all personal information data elements involved; the use of some personal information data

elements may have a different authority than other personal information data elements. Check all that apply.

☐ The personal information is being used under this Initiative according to the original purpose for which it was collected or compiled or for a use that is consistent with that original purpose of collection. [s. 39(1)(a)]

If the above is selected and the use includes consistent purposes, please confirm the consistent use meets both of the following:

☐ The consistent use has a reasonable and direct connection to the purpose for which the personal information was originally collected or compiled.

AND

☐ The consistent use is necessary for performing the statutory duties of or operating a legally authorized program of the public body using the personal information.

Provide details/explanation:

☐ The individual has identified the information and consented to the use. [s. 39(1)(b)]

Consent has specific requirements for validity whether in writing, electronic or oral. Please discuss the requirements for valid consent with your FOIP Office.

☐ The use is for a purpose for which the information was disclosed to the public body under section 40, 42 or 43 of the FOIP Act. [s. 39(1)(c)]

If the above is selected and another public body is disclosing personal information to this Initiative under a FOIP Act disclosure authority (sections 40, 42 or 43), this is the corresponding authority for the Initiative's use of the information.

*If this Initiative receives and uses personal information disclosed from another public body and you are uncertain it is being disclosed under the FOIP Act, you may wish to return to this question after reviewing the authorities in **Disclosure** beginning at Part 6 of this assessment and in consultation with the other public body.*

If you have checked one of the preceding authorities for use, you have identified an authority under the FOIP Act that allows the Initiative to use the personal information. Please continue the assessment.
If none of these use authorities is selected, you have not identified an authority under the FOIP Act that allows the Initiative to use the personal information. **Please contact your FOIP Office for assistance.**

Part Six: Disclosure for research or statistical purposes (section 39)

Has a researcher requested records that contain personal information as part of this initiative? **Yes/No**

If the answer is YES, then all the conditions under section 42 of the FOIP Act must be met including signing an agreement to comply with the approved conditions. **Please contact your FOIP Office for assistance.**
If the answer is YES, and this is the only disclosure, go to *Accuracy and Retention* under Part 9 of this assessment.
If the answer is YES, and there may be additional disclosure authorities, or if the answer is NO, go to *Disclosure of Information in Archives* under Part 7 of this assessment.

Part Seven: Disclosure of information in archives (section 43)

The Provincial Archives of Alberta and the archives of a public body may disclose information as authorized by section 43 of the FOIP Act.

Is the disclosure of personal or other information held in an archives part of this Initiative? **Yes/No**

If the answer is YES, continue under this part of the assessment.
If the answer is NO, go to *Disclosure of Personal Information* under Part 8 of this assessment.

☐ Has the record been in existence for 25 years or more and the disclosure would not be an unreasonable invasion of privacy under section 17 of the FOIP Act? [s. 43(1)(a)(i)(A) with s. 17]

☐ Has the record been in existence for 25 years or more and the disclosure is for research or statistical purposes in accordance with section 42 of the FOIP Act? [s. 43(1)(a)(i)(B) with s. 42]

☐ Has the record been inexistence for 75 years or more? [s. 43(1)(a)(ii)]

☐ Has the record been in existence for 25 years or more and the disclosure would not be harmful to the business interests of a third party under section 16 of the FOIP Act? [s. 43(1)(b)(i) with s. 16]

☐ Has the record been in existence for 25 years or more and the disclosure would not be harmful to a law enforcement matter within the meaning of section 20 of the FOIP Act? [s. 43(1)(b)(ii) with s. 20]

☐ Has the record been in existence for 25 years or more and the information is not subject to any type of legal privilege under section 27 of the FOIP Act? [s. 43(1)(b)(iii) with s. 27]

If you have checked one or more of these authorities for Disclosure of Information in Archives and this is the only disclosure is archival, go to *Accuracy and Retention* under Part 9 of this assessment.
If there are other disclosures, or if no authorities listed above apply, go to *Disclosure of Personal Information* under Part 8 of this assessment.

Part Eight: Disclosure of personal information (section 40)

Is the Initiative disclosing personal information? **Yes/No**

If the answer is YES, continue under this part of the assessment.
If the answer is NO, go to *Accuracy and Retention* under Part 9 of this assessment.

There are many authorities that allow for a public body to disclose personal information under the FOIP Act. Please think about all personal information data elements disclosed and all instances of disclosure; the disclosure of some personal information data elements may have a different authority than other personal information data elements. Additionally, a disclosure to one public body or organization may have a different authority than a disclosure to another one.

Section 40(4) requires that a public body may disclose personal information only to the extent necessary to enable the public body to the carry out the purposes (described in the disclosure provisions that follow) in a reasonable manner.

Check only those types of disclosure that are specifically intended to occur under the Initiative under assessment.

☐ The disclosure is in accordance with a FOIP Act access request. [s. 40(1)(a)]

☐ The disclosure is not an unreasonable invasion of a third party's privacy under s. 17. [s. 40(1)(b) with s. 17]

Note: Section 17(2) lists when a disclosure is not an unreasonable invasion of privacy under formal access. If disclosure under this Initiative is listed in section 17(2), then this disclosure provision may apply.

☐ The personal information is being disclosed under this Initiative according to the original purpose for which it was collected or compiled or for a use that is consistent with that original purpose of collection. [s. 40(1)(c)]

If the above is selected and the use includes consistent purposes, please confirm the consistent use meets both of the following:

☐ The consistent use has a reasonable and direct connection to the purpose for which the personal information was originally collected or compiled.

AND

☐ The consistent use is necessary for performing the statutory duties of or operating a legally authorized program of the public body using the personal information.

Provide details/explanation:

☐ The individual has identified the information and consented to the disclosure in the prescribed manner. [s. 40(1)(d)]

Consent has specific requirements for validity whether in writing, electronic or oral. Please discuss the requirements for valid consent with your FOIP Office.

☐ The disclosure is done in order to comply with an enactment of Alberta or Canada, or with a treaty, arrangement or agreement made under an enactment of Alberta or Canada. [s. 40(1)(e)]

☐ The disclosure is for any purpose where an enactment of Alberta or Canada authorizes or requires the disclosure. [s. 40(1)(f)]

☐ The disclosure is to comply with a subpoena, warrant or order made by a court, person or body having jurisdiction in Alberta to compel the production of information or with a rule of court binding in Alberta that relates to the production of information. [s. 40(1)(g)]

☐ The disclosure is to an officer or employee of the public body or to a member of the Executive Council, and is necessary for the performance of the duties of that officer, employee or member. [s. 40(1)(h)]

☐ The disclosure is to an officer or employee of a public body or to a member of Executive Council, if the disclosure is necessary for the delivery of a common or integrated program or service and the performance of the duties of the officer or employee or member to whom the information is disclosed. [s. 40(1)(i)]

☐ The disclosure is for the purpose of enforcing a legal right that the Government of Alberta or a public body has against any person. [s. 40(1)(j)]

☐ The disclosure is for the purpose of:

i) Collecting a fine or debt owing by an individual to the Government of Alberta or to a public body, or to an assignee of either of them, [s. 40(1)(k)(i)] or

ii) Making a payment owing by the Government of Alberta or a public body to an individual. [s. 40(1)(k)(ii)]

☐ The disclosure is for the purpose of determining or verifying an individual's suitability or eligibility for a program or benefit. [s. 40(1)(l)]

☐ The disclosure is to the Auditor General or any other prescribed person or body for audit purposes. [s. 40(1)(m)]

☐ The disclosure is to a member of the Legislative Assembly who has been requested by the individual the information is about to assist is resolving a problem. [s. 40(1)(n)]

☐ The disclosure is to a representative of a bargaining agent who has been authorized in writing by the employee the information is about to make an inquiry. [s. 40(1)(o)]

☐ The disclosure is to the Provincial Archives of Alberta or to the archives of a public body for permanent preservation. [s. 40(1)(p)]

☐ The disclosure is to a public body or a law enforcement agency in Canada to assist in an investigation:

i) Undertaken with a view to a law enforcement proceeding, [s. 40(1)(q)(i)] or

ii) From which a law enforcement proceeding is likely to result. [s. 40(1)(q)(ii)]

☐ The disclosure is from a law enforcement agency and the information is disclosed:

i) To another law enforcement agency in Canada, [s. 40(1)(r)(i)] or

ii) To a law enforcement agency in another country under an arrangement, written agreement, treaty or legislative authority. [s. 40(1)(r)(ii)]

Note: law enforcement is defined under section 1(h) of the FOIP Act. In order to apply this authority, please review this definition and Bulletin No. 7: Law Enforcement found at: http://www.servicealberta.gov.ab.ca/foip/resources/bulletins.cfm

☐ The disclosure is so that the spouse or adult interdependent partner, relative or friend of an injured, ill or deceased individual may be contacted. [s. 40(1)(s)]

☐ The disclosure is in accordance with s. 42 (Disclosure for Research or Statistical Purposes) or 43 (Disclosure of Information in Archives). [s. 40(1)(t) with s. 42 or s. 43]

*If **YES**, see also **Disclosure for Research or Statistical Purposes** and/or **Disclosure of Information in Archives** under Parts 6 and 7 of this assessment.*

☐ The disclosure is to an expert for the purposes of s. 18(2). [s. 40(1)(u) with s. 18(2)]

Section 18(2) applies under formal access when disclosure may be harmful to individual or public safety and the personal information of the applicant must be disclosed to an expert in order for their assessment to determine if section 18 applies.

☐ The disclosure is for use in a proceeding before a court or quasi-judicial body to which the Government of Alberta or a public body is a party. [s. 40(1)(v)]

☐ The disclosure is by the Minister of Justice and Solicitor General or an agent or lawyer of the Minister of Justice and Solicitor General to a place of lawful detention. [s. 40(1)(w)]

☐ The disclosure is for the purpose of managing or administering personnel of the Government of Alberta or the public body. [s. 40(1)(x)]

☐ The disclosure is to the Director or Maintenance Enforcement for the purpose of enforcing a maintenance order under the *Maintenance Enforcement Act*. [s. 40(1)(y)]

☐ The disclosure is to an officer of the Legislature, if the information is necessary for the performance of the duties of that officer. [s. 40(1)(z)]

☐ The disclosure is for the purpose of supervising an individual under the control or supervision of a correctional authority. [s. 40(1)(aa)]

☐ The Initiative is disclosing personal information that is available to the public. [s. 40(1)(bb)]

☐ The Initiative is disclosing personal information that is routinely disclosed in a business or professional context, i.e. limited to an individual's name and business contact information, including business title, address, telephone number, facsimile number and e-mail address and does not reveal other personal information about the individual or personal information about another individual. [s. 40(1)(bb.1)]

☐ The disclosure is to the surviving spouse or adult interdependent partner of a relative of a deceased individual if, in the opinion of the head of the public body, the disclosure is not an unreasonable invasion of the deceased's personal privacy. [s. 40(1)(cc)]

☐ The disclosure is to a lawyer or student-at-law acting for an inmate under the control or supervision of a correctional authority. [s. 40(1)(dd)]

☐ The head of the public body believed, on reasonable grounds, that the disclosure will avert or minimize a risk of harm to the health or safety of a minor. [s. 40(1)(ee)(i)]

☐ The head of the public body believed, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person. [s. 40(1)(ee)(ii)]

☐ The disclosure is to the Administrator of the *Motor Vehicle Accident Claims Act* or to an agent or lawyer of the Administrator for the purpose of dealing with claims under that Act. [s. 40(1)(ff)]

☐ The disclosure is to a law enforcement agency, an organization providing services to a minor, another public body or any prescribed person or body if the information is in respect of a minor or a parent or guardian of a minor and the head of the public body believes, on reasonable grounds, that the disclosure is in the best interests of that minor. [s. 40(1)(gg)]

Additional provisions related to post-secondary educational bodies are in place. If this PIA is being completed by a post-secondary institute, please check with your FOP Office.

If you checked at least one of the preceding authorities for disclosure, you have identified an authority under the FOIP Act that allows the Initiative to disclose the personal information. Please continue the assessment.
If the answer is NO to all of these disclosure authorities above, you have not identified an authority under the FOIP Act that allows the Initiative to disclose the personal information. Please contact your FOIP Office for assistance.

Part Nine: Accuracy and retention (section 35)

If an individual's personal information is used by a public body to make a decision that directly affects the individual, the public body must make every reasonable effort to ensure that the information is accurate and complete.

An individual has a right to access their personal information for a period of one year after it is used to make a decision that directly affects them. A shorter retention period may be agreed upon by the individual, the public body and any other body that approves retention schedules. Or there may be longer retention periods required due to business and legal requirements.

It is important that you ensure an appropriate records retention and disposition schedule is applied. Alberta government records cannot be destroyed or archived without a records retention and disposition schedule in place. This increases risk in storing records longer than may be required and potentially increases the volume of responsive records under a formal access request.

Do you have an approved records retention and disposition schedule for the records subject to this initiative? [s. 35(a)] *If yes, please provide the records retention and disposition schedule number or name:*

If the answer is NO, or if you are uncertain, please contact the individual(s) responsible for records management in your public body.

This is not a PIA requirement but another business consideration.

Are there procedures in place to enable an individual to request/review a copy of their own personal information? [s. 35(b)]

If the answer is NO, or if you are uncertain, please contact your FOIP Office for assistance: *http://www.servicealberta.ca/foip/directory-of-public-bodies.cfm*

Part Ten: Correction and personal information (section 35)

If an individual believes there is an error or omission in their personal information, they have the right to request correction.

The public body must not correct an opinion such as professional or expert opinions.

Annotation or Linking: if the correction is not made or cannot be made, the request for correction must be annotated or linked to the record.

*Note: **Annotate** means written on a record close to the information. **Link** means attach to, join or connect to the original record.*

Check all that apply.

☐ There are procedures in place to correct, annotate or link an individual's personal information if requested, including what source was used to update the file. [ss. 36(1), (2), (3) and (6)]

☐ If personal information is corrected, are there procedures in place to notify other holders of this information in accordance with the FOIP Act? [ss. 36(4) and (5)]

☐ Are there procedures in place to give written notice to the individual when a correction, annotation or linkage has been made to an individual's personal information? [s. 36(6)]

☐ Are there procedures in place to transfer a request for correction to another public body and notify the individual of the transfer? [s. 15]

If you have not checked all boxes in *Correction of Personal Information* under Part 10 of this assessment is *NO*, please contact your FOIP Office for assistance: *http://www.servicealberta.ca/foip/directory-of-public-bodies.cfm*

Part Eleven: Security and storage for the protection of personal information (section 38)

A public body is required to protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. This PIA Questionnaire is not a security assessment, nor a threat and risk assessment.

Please complete this part of the assessment with the understanding that ideally this section should be completed in collaboration with the information security office of your public body, or individuals responsible for information security, who can advise in relation to risk and vulnerability. The head of the public body, or their delegate, is responsible to ensure personal information is protected under the FOIP Act.

The "Business Owner" or "Custodian" with day-to-day responsibility for the information is accountable for any risk to the security of the confidential and personal information captured under this Initiative or under the scope of this PIA.This accountability to the head of a public body, or their delegate, must be considered and understood on the part of the program area and signatories signing off on this PIA.

If your public body does not have an information security policy, it is a good idea to develop one based on current industry standards, with consideration to the type and sensitivity of the information in your public body's custody and control. Sometimes these security measures may be simple physical ones (such as locking a cabinet) or administrative (such as training) or technical. For further direction, please refer to the list of security resources attached, in consultation with your public body's information security or information technology resources.

Does this Initiative comply with your public body's information security management policies, rules and procedures? [s.38] **Yes/No**

If the answer is YES, please continue with the assessment.
If the answer is NO, you have not satisfied the security requirement of this PIA. Please contact your information security office for assistance.

How is the information involved in this Initiative classified for security purposes?

Your public body may have its own information security classification and if it does, you should apply that classification. If not, you may wish to adapt the Government of Alberta classification system to the types of information in your public body. GoA information is classified according to the Information Security Classification which can be found at:

http://imtdocs.alberta.ca/Information_Security_Classification_v2.pdf

Please provide or describe the information classification. If you have any questions regarding the classification please contact your records management or information security office.

Provide Program Area Security Contact Information.

This should be the name of the individual able to respond to questions about meeting reasonable security measures under this Initiative.

Name/Title	
Branch/Unit	

Telephone	
E-Mail	

Additional Comments:

Part Twelve: Signatures

Suggested Signatures with Signatories names printed and date of signature.

Signature: _____ Date: _____

Program Area – responsible to provide information in this PIA related to the Initiative that is complete and accurate.

Signature: _____ Date: _____

FOIP Office – provides support in understanding the PIA Questionnaire and meeting FOIP Act requirements.

Signature: _____ Date: _____

Information Security Office or individual responsible for overseeing information security – provides support in understanding compliance with GoA security directives.

Signature: _____ Date: _____

Head of a Program Area or Executive – someone with accountability for the program and/or records, i.e. “business owner”.

Security Resources and Industry Standards

Provincial agencies, boards and commissions are subject to the GoA Information Security Directives and can use those as a guide. Local public bodies can establish their own information security policies. The following are industry standards to provide guidance to those policies.

International Standards Organization (ISO) Standards

- ISO 27001 (Information Security Management) http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
- ISO 27002 (Code of Practice, Information Security Controls) http://www.iso.org/iso/catalogue_detail?csnumber=54533
- ISO 22301 (Business Continuity) http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50038

Other Important Standards and Frameworks

- National Institute of Standards and Technology (NIST) http://www.nist.gov/information-technology-portal.cfm
- Payment Card Industry Data Security Standards (PCI-DSS) https://www.pcisecuritystandards.org/security_standards Required when taking credit card payments.
- Information Technology Infrastructure Library (ITIL) Framework for IT Service Management http://www.itil.org.uk
- Control Objectives for Information and Related Technology (COBIT) Framework http://www.isaca.org/cobit/pages/default.aspx

Web App Security Organizations and Standards

- Open Web Application Security Project (OWASP) https://www.owasp.org/index.php/Main_Page
- Web Application Security Consortium (WASC) http://www.webappsec.org
- World Wide Web Consortium (W3C) http://www.w3.org/standards