

Protection of Privacy

ATIPP Act: Part IV

POLICY & PROCEDURES MANUAL

January 2008



Justice

ACCESS TO INFORMATION AND PROTECTION OF PRIVACY

Coordinating Office

Table of Contents

| | | |
|-------------|------------------------------------------------------------------|-----------|
| 5 | ATIPP ACT – PROTECTION OF PRIVACY | 4 |
| 5.1 | Fair Information Practices | 5 |
| 5.2 | Definition of Personal Information | 6 |
| 5.3 | Purpose for which Personal Information may be Collected | 7 |
| 5.3.1 | What does ‘Collection’ mean? | 7 |
| 5.3.2 | Minimum amount of information to be collected | 7 |
| 5.3.3 | Collection by external contractors | 7 |
| 5.4 | How Personal Information is to be Collected | 8 |
| 5.4.1 | Direct collection | 9 |
| 5.4.2 | Indirect collection | 9 |
| 5.4.3 | Privacy Notice | 12 |
| 5.5 | Accuracy of Personal Information | 13 |
| 5.6 | Right to Request Correction of Personal Information | 14 |
| 5.6.1 | Making a correction or annotation | 14 |
| 5.6.2 | Duty to inform other public bodies or organizations | 15 |
| 5.6.3 | Timing for making a decision about a correction or annotation | 15 |
| 5.7 | Protection of Personal Information | 16 |
| 5.7.1 | Physical safeguards | 16 |
| 5.7.2 | Administrative safeguards | 16 |
| 5.7.3 | Security and technical safeguards | 17 |
| 5.8 | Retention of Personal Information | 18 |
| 5.9 | Use of Personal Information | 19 |
| 5.9.1 | Use for original purpose or consistent purpose | 19 |
| 5.9.2 | Individual has identified the information & consented to its use | 20 |
| 5.9.3 | Use consistent with sections 39-42 | 20 |
| 5.9.4 | Minimum amount of information to be used | 20 |
| 5.10 | Disclosure of Personal Information | 21 |
| 5.10.1 | Discretion to disclose | 22 |
| 5.10.2 | Minimum amount of information to be disclosed | 23 |
| 5.10.3 | Request for disclosure | 23 |
| 5.10.4 | Consent to disclosure from the individual | 23 |
| 5.10.5 | Disclosure for Research or Statistical Purposes | 25 |
| 5.10.6 | Disclosure for Archival or Historical Purposes | 26 |
| 5.10.7 | Disclosure to a Member of the House of Assembly | 26 |

| | | |
|-------------------------------------------------------------|--------------------------------------------------------|------------|
| 5.11 | Privacy Tools for Assessing Compliance | 27 |
| 5.11.1 | Annual Privacy Checklist..... | 28 |
| 5.11.2 | Privacy Impact Assessment (PIA) Protocol..... | 30 |
| 5.12 | Privacy Breaches | 36 |
| 5.12.1 | What is a privacy breach? | 36 |
| 5.12.2 | Consequences of a privacy breach | 36 |
| 5.12.3 | Examples of a privacy breach | 36 |
| 5.12.4 | Four key steps in responding to a privacy breach | 37 |
| Appendix A: Information Sharing Agreement (ISA)..... | | 41 |
| Appendix B: Generic Privacy Notice | | 45 |
| Appendix C: Annual Privacy Checklist | | 46 |
| Appendix D: PIA Policy..... | | 56 |
| Appendix E: PIA Protocol | | 67 |
| Appendix F: Preliminary PIA..... | | 69 |
| Appendix G: PIA Template (Annotated) | | 81 |
| Appendix H: Privacy Breach Protocol..... | | 123 |

5 ATIPP Act – Protection of Privacy

The Government of Newfoundland and Labrador is responsible for extensive amounts of personal information. Part IV of the *ATIPP Act* seeks to protect this personal information by limiting how personal information can be collected, used and disclosed by public bodies. The privacy provisions also allow individuals the right to access and correct their personal information.

Part IV of the *ATIPP Act* is made up of *sections 32 - 42*. For the exact wording of these sections, please see *Appendix 4* of this Manual. To view an online version of the *ATIPP Act*, please visit the House of Assembly website:

<http://www.hoa.gov.nl.ca/hoa/statutes/a01-1.htm>

The Privacy provisions of the *ATIPP Act* include the following sections:

- (32) Purposes for which information may be collected**
- (33) How personal information is to be collected**
- (34) Accuracy of personal information**
- (35) Right to request correction of personal information**
- (36) Protection of personal information**
- (37) Retention of personal information**
- (38) Use of personal information**
- (39) Disclosure of personal information**
- (40) Definition of consistent purposes**
- (41) Disclosure for research or statistical purposes**
- (42) Disclosure for archival or historical purposes**

These sections are also informed by the definitions contained in *section 2*, particularly the definition of ‘**personal information**’ in *section 2(o)*.

The ATIPP Office has developed a number of tools to help Government departments and other public bodies comply with the privacy provisions, including:

- *Annual Privacy Checklist*
- *Preliminary Privacy Impact Assessment (PIA) Checklist*
- *Privacy Impact Assessment Template*
- *Privacy Breach Protocol*

These privacy tools are discussed in detail later in this Chapter.

5.1 Fair Information Practices

The *ATIPP Act* privacy provisions are based on standards for privacy protection developed by the Canadian Standards Association (CSA), known as the 'Fair Information Practices'. The CSA is a not-for-profit organization which develops standards to address the needs of business, industry, government and consumers. The Fair Information Practices are:

1) Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles;

2) Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected;

3) Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate;

4) Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means;

5) Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes;

6) Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used;

7) Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information;

8) Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information;

9) Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate; and

10) Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

5.2 Definition of Personal Information

The privacy provisions of the *ATIPP Act* apply only to personal information. Personal information is defined in the *ATIPP Act* as follows:

- 2 (o) **personal information** means recorded information about an identifiable individual, including
- i) The individual's name, address or telephone number;
 - ii) The individual's race, national or ethnic origin, color, or religious or political beliefs or associations;
 - iii) The individual's age, sex, sexual orientation, marital status or family status;
 - iv) An identifying number, symbol or other particular assigned to the individual;
 - v) The individual's fingerprints, blood type or inheritable characteristics;
 - vi) Information about the individual's health care status or history, including a physical or mental disability;
 - vii) Information about the individual's educational, financial, criminal or employment status or history;
 - viii) The opinions of a person about the individual, and
 - ix) The individual's personal views or opinions.

It is important to note that while Section 2(o)(i-ix) gives examples, it is not an exhaustive list of personal information.

5.3 Purpose for which Personal Information may be Collected

Section 32 limits the circumstances whereby a public body may collect personal information:

- 32 No personal information may be collected by or for a public body unless
- a) The collection of that information is expressly authorized by or under an Act;
 - b) That information is collected for the purposes of law enforcement; or
 - c) That information relates directly to and is necessary for an operating program or activity of the public body.

Personal information should not be collected for any other purposes – if a public body does not meet the above criteria when collecting personal information, under the *ATIPP Act* they should not be collecting that information.

5.3.1 What does ‘Collection’ mean?

In reference to the *ATIPP Act*, a public body ‘collects’ personal information whenever the public body compiles or creates a record of personal information. This includes, but is not limited to, personal information that is:

- gathered by the public body in forms, interviews, or correspondence;
- provided to the public body by another public body;
- collected by a contractor or other third party on behalf of the public body; and
- in correspondence received by the public body, including unsolicited letters and resumes.

‘Collection’ is not restricted to any particular method, media, or technology. Personal information may be collected in writing, by audio or video, with any electronic or other media, etc...

5.3.2 Minimum amount of information to be collected

Where personal information is collected because it relates to an operating program or activity (*section 32(c)*), public bodies should ensure the information is necessary. The collection should be limited to the minimum amount of information needed to achieve the purpose of the collection.

For example, if only the name and telephone number of a person is required for a program, then address and social insurance number should not be collected. Public bodies should review their forms to ensure only necessary information is being collected.

5.3.3 Collection by external contractors

Collection of personal information may be carried out by the public body itself, by another public body, or by an outside organization (such as a contractor) on behalf of the public body. A public body is bound by the requirements of the *ATIPP Act* whether it collects the personal information itself or authorizes another party to collect on its behalf.

Where an outside agent or organization is collecting personal information on behalf of a public body, the public body should have a written agreement in place to ensure the personal information is properly protected when in the custody of another party. The agreement should address such matters as use, security, retention and disclosure of the personal information.

For additional information related to formalized agreements for the sharing of personal information, see [Appendix A: Information Sharing Agreement \(ISA\)](#).

5.4 How Personal Information is to be Collected

Section 33 of the ATIPP Act stipulates how public bodies must collect personal information:

- 33 (1) *A public body shall collect personal information directly from the individual the information is about unless*
- a) *another method of collection is authorized by*
 - i) *that individual, or*
 - ii) *an Act or regulation;*
 - b) *the information may be disclosed to the public body under sections 39 to 42; or*
 - c) *the information is collected for the purpose of*
 - i) *determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary,*
 - ii) *an existing or anticipated proceeding before a court or a judicial or quasi-judicial tribunal,*
 - iii) *collecting a debt or fine or making a payment,*
 - iv) *law enforcement, or*
 - v) *Collection of the information is in the interest of the individual and time circumstances do not permit collection directly from the individual.*
- 33 (2) *A public body shall tell an individual from whom it collects personal information*
- d) *the purpose for collecting it;*
 - e) *the legal authority for collecting it; and*
 - f) *the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.*
- 33 (3) *Subsection (2) does not apply where*
- g) *the information is about law enforcement or anything referred to in section 22(1) or*
 - h) *in the opinion of the head of the public body complying with it would*
 - i) *result in the collection of inaccurate information, or*
 - ii) *Defeat the purpose or prejudice the use for which the information is collected.*

5.4.1 Direct collection

As stated in *Section 33 (2)* of the *ATIPP Act*, public bodies should collect personal information directly from the individual who is the subject of that information.

There are advantages to direct collection. First, direct collection ensures individuals are aware of the information being collected. Direct collection also gives the public body a clear opportunity to inform the individual how the information will be used and to whom it will be disclosed.

Secondly, direct collection allows public bodies to ensure information is as accurate as possible. Collecting information directly from the person makes it more likely that the information is accurate. For example, it is unlikely that an individual would incorrectly state his or her date of birth.

When personal information is being collected directly from an individual, *Section 33 (2)* of the *ATIPP Act* states:

33 (2) A public body shall tell an individual from whom it collects personal information

- a) the purpose for collecting it;*
- b) the legal authority for collecting it; and*
- c) the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.*

This notification to the individual is known as the 'privacy notice'. For more information, see section [5.4.3 Privacy Notice](#).

5.4.2 Indirect collection

Even though direct collection is always preferred, *Section 33* of the *ATIPP Act* does provide some exceptions to direct collection.

Indirect collection means personal information is being obtained from someone other than the person the information is about. *Section 33(1)* allows indirect collection of personal information in specific circumstances.

Please note that where information is collected indirectly, the purpose of the collection must still comply with *Section 32* of the *ATIPP Act*.

5.4.2.1 Indirect collection authorized by the individual

33 (1) public body shall collect personal information directly from the individual the information is about unless

- a) another method of collection is authorized by*
 - (i) that individual,*

Information can be collected indirectly if the collection is authorized by the individual. Such authorization should be in writing, if possible. If authorization must be given verbally, the public body should document the conversation and send a letter to the individual confirming the authorization.

5.4.2.2 Indirect collection authorized by an Act or Regulation

- 33 (1) *A public body shall collect personal information directly from the individual the information is about unless*
- ii) *an Act or regulation;*

Where this section is used to justify an indirect collection, the legislation should describe the type of personal information to be collected.

Where legislation allows indirect collection, the collection should be limited to the kinds of information specified in the Act or regulation, even where indirect collection is allowed, the personal information collected should be limited to only that information which is necessary.

5.4.2.3 Indirect collection authorized under sections 39 - 42

- 33 (1) *A public body shall collect personal information directly from the individual the information is about unless*
- c) *the information may be disclosed to the public body under sections 39 to 42*

Sections 39-42 of the ATIPP Act set out the circumstances where public bodies may disclose personal information. Section 33(1)(b) allows public bodies to receive or “collect” information that is disclosed under these sections, which include:

- *Disclosure of personal information (S. 39)*
- *Disclosure for research or statistical purposes (S. 41)*
- *Disclosure for archival or historical purposes (S. 42)*

5.4.2.4 Indirect collection authorized under section 33(1)(c)

- 33 (1) *A public body shall collect personal information directly from the individual the information is about unless*
- c) *the information is collected for the purpose of*
 - i) *determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary,*
 - ii) *an existing or anticipated proceeding before a court or a judicial or quasi-judicial tribunal,*
 - iii) *collecting a debt or fine or making a payment,*
 - iv) *law enforcement, or*
 - v) *Collection of the information is in the interest of the individual and time circumstances do not permit collection directly from the individual.*

Section 33(1)(c) allows indirect collection of personal information for a number of purposes:

Suitability for an honour or award

A public body may collect personal information indirectly for determining the individual's suitability for an honour or award. This provision allows a public body to collect such information where it is considering granting an honour or award on an individual without the individual's knowledge. This clause of the ATIPP Act lists some examples of honours and awards – a honorary degree, scholarship, prize or bursary – but this is not an exhaustive list.

Proceeding before a court or tribunal

A public body may collect personal information indirectly if the information is for a proceeding before a court or tribunal. Examples of such proceedings include:

- *A court proceeding in which a person is charged with a criminal offence*
- *A civil proceeding (e.g. where a citizen is bringing a lawsuit against a Department)*
- *A hearing before the Human Rights Commission*
- *A hearing before the Labour Relations Board*

If you are unsure about whether a particular proceeding falls under this section, please consult your Department's solicitor.

Collecting a debt or payment of money

Where a public body is collecting a debt or fine owing to it or to the Government of Newfoundland and Labrador, it is permitted to collect information indirectly. This may be necessary where the public body cannot locate the individual or believes it would not obtain complete or accurate information from the individual, etc.

A 'payment' is a sum of money that the Government of Newfoundland and Labrador owes to an individual. *Clause 33(1)(c)(iii)* permits the public body to obtain personal information indirectly to enable the public body to make the payment. Usually, this situation will arise when the individual has moved and the public body does not have a forwarding address, or where the public body is trying to verify the identity of the individual in order to make the payment.

Law enforcement

Indirect collection of personal information is permitted for law enforcement purposes. As defined in the ATIPP Act:

- (2) (i) *"law enforcement" means*
- i) policing, including criminal intelligence operations, or*
 - ii) investigations, inspections or proceedings that lead or could lead to a penalty or sanction being imposed.*

Collection is in the individual's interest

A public body is permitted to collect information indirectly where the collection of information is in the interest of an individual. There are two requirements:

- *Collection of the personal information must be in the interest of the individual who is the subject of that information. In other words, there must be some benefit to the individual resulting from the collection of the personal information, and*
- *Time or circumstances do not permit collection of the personal information directly from the individual. (e.g., there is some element of urgency)*

For example, suppose an individual is involved in a workplace accident and is unconscious. The department may obtain the next of kin from their records and provide that personal information the hospital.

5.4.3 Privacy Notice

33 (2) *A public body shall tell an individual from whom it collects personal information*

- a) *the purpose for collecting it;*
- b) *the legal authority for collecting it; and*
- c) *the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.*

5.4.3.1 Written privacy notice

Section 33(2) outlines the **privacy notice**, which is the required information given to an individual where a public body is collecting personal information directly from that individual. Privacy notices should be in writing, where possible. Any forms used to collect personal information should contain a privacy notice.

The legal authority for the collection, required by section 33(2)(b) may be found in an Act (including the *ATIPP Act*), a regulation, a contractual agreement, court order, etc... If you are not sure if you have legal authority to collect the information, please contact your Department's solicitor.

Where a variety of personal information is collected, the notice should state the purpose and authority for all pieces of information. If there are two different purposes for collection, both purposes should be described in the privacy notice. For examples of written privacy notices, see [Appendix B: Generic Privacy Notice](#).

5.4.3.2 Verbal privacy notice

A written privacy notice may not always be possible. For example, a public body may need to collect information on an urgent basis but the individual may live outside the area and may not have access to a fax machine. When verbal notice is used, it should contain the same required information as the written privacy notice would contain – the purpose for collection; the authority for collection; and the contact information of an employee who can answer questions about that collection of personal information.

A verbal privacy notice should be provided at the beginning of the conversation, before the information is collected. If the public body gives notice verbally, the public body should follow up with a letter confirming the verbal privacy notification.

5.4.3.3 Where privacy notice is not required

33 (3) *Subsection (2) does not apply where*

- a) *the information is about law enforcement or anything referred to in section 22(1) or*
- b) *in the opinion of the head of the public body complying with it would*
 - i) *result in the collection of inaccurate information, or*
 - ii) *Defeat the purpose or prejudice the use for which the information is collected.*

Section 22, referenced in this clause, refers to circumstances where a public body is not required to release information. The decision not to include a privacy notice because it would lead to inaccurate information, or would prejudice the information, must be made by the head of the public body, or the appropriate delegated authority.

Under section 33(3)(b), a privacy notice is not required where providing notification would defeat the purpose of the collection.

5.5 Accuracy of Personal Information

34 *Where an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body shall make every reasonable effort to ensure that the information is accurate and complete.*

Section 34 places the onus on public bodies to ensure the personal information they use to make a decision directly affecting an individual is accurate and complete.

This requirement is limited to situations where the personal information will be used to “make a decision that directly affects the individual.” Examples include determining if an individual is entitled to a benefit such as social assistance or determining if an individual will be offered a job with the public service.

The meaning of “**reasonable effort**” will depend on the circumstances, and may include:

- *conducting periodic checks, directly with the individual or using other authorized avenues, to ensure the information is still current and valid;*
- *undertaking thorough reviews of applications to ensure all questions are answered completely (e.g. applications for employment or social assistance);*
- *documenting when personal information is collected or received, and*
- *implementing processes for correcting personal information.*

5.6 Right to Request Correction of Personal Information

Section 35 of the *ATIPP Act* gives applicants the right to ask a public body to correct their personal information where it is wrong or to provide additional information where it is incomplete. This section also sets out the procedure for making such corrections to personal information.

- 35 (1) *An applicant who believes there is an error or omission in his or her personal information may request the head of the public body that has the information in its custody or under its control to correct the information.*
- (2) *Where no correction is made in response to a request under subsection (1), the head of the public body shall annotate the information with the correction that was requested but not made.*
- (3) *Where personal information is corrected or annotated under this section, the head of the public body shall notify a public body or a third party to whom that information has been disclosed during the one-year period before the correction was requested.*
- (4) *Where a public body is notified under subsection (3) of a correction or annotation of personal information, the public body shall make the correction or annotation on a record of that information in its custody or under its control.*
- (5) *A request under this section shall be in writing.*
- (6) *Within 30 days after receiving a request under this section, the head of a public body shall*
- (a) Make the requested correction and notify the applicant of the correction; or*
- (b) Notify the applicant of the head's refusal to correct the record and the reason for the refusal, that the record has been annotated, and that the applicant may ask for a review of the refusal under Part V.*

5.6.1 Making a correction or annotation

Section 35 requires public bodies to make corrections to an applicant's personal information if the individual can demonstrate it is inaccurate or incomplete. Even if no correction or addition is made, the record must be annotated.

Not all requests for correction of personal information need to be, or should be, made under section 35 of the *ATIPP Act*. This section does not replace existing procedures under which an individual can request correction of personal information in a record; nor does section 35 prevent a public body from correcting personal information that is clearly incorrect or out of date. However, even if a correction is handled informally, it is a good practice to ensure such corrections are included in the original file.

5.6.1.1 Request for correction of factual information

When a request for a factual correction is received, the public body should assess the request. If the applicant gives adequate proof that the information held by the public body is incorrect or incomplete, a correction should be made. Even where proof is inadequate, the record should be annotated.

Where the public body determines a correction should be made, the public body should correct the record by clearly marking the original information as incorrect and attaching the correct information to the records.

Where the personal information is incomplete, the public body should add the additional information, provided there is adequate proof. Where there is inadequate proof to make a

correction, the public body must still annotate the information. This can be done by adding explanatory notes, letters, reports, or other information to the file. For example, an annotation may consist of a letter or written statement in which the applicant disputes the facts as presented or disagrees with an opinion previously expressed by the applicant or another person about the applicant.

5.6.1.2 Request for correction of opinion information

Sometimes information in a record is based on an opinion. For example, a record may contain an assessment of a person's abilities, performance, or other characteristics. Because opinions are subjective, they usually cannot be corrected. In these circumstances, public bodies must annotate the record with a statement that the applicant does not agree with the opinion previously given. If the opinion is based on inaccurate or incorrect information, and the information is used to make a decision affecting the individual, the public body should ask the person who supplied the opinion to provide an amended opinion.

5.6.1.3 Include correction or annotation with original file

Whenever a correction or an annotation is made, the file should be set up so that the correction or annotation will always be retrieved when the original file is retrieved.

5.6.2 Duty to inform other public bodies or organizations

If a correction or annotation is made, the public body should determine if any other public bodies or third parties have received the information in the past year. If so, the public body should inform the public bodies or third parties about the correction or annotation. A year runs from the date the correction was requested.

Where a public body *receives* information about a correction or annotation, it is required to make the correction on their own files as well. Individuals or organizations not covered by the *ATIPP Act* cannot be compelled to correct/annotate their records but they must be notified by the public body.

As normal practice, a record should be kept of all disclosures of personal information to other public bodies and third parties, enabling subsequent notification of a correction or annotation to the record.

5.6.3 Timing for making a decision about a correction or annotation

35 (6) *Within 30 [calendar] days after receiving a request under this section, the head of a public body shall*

(a) make the requested correction and notify the applicant of the correction; or

(b) notify the application of the head's refusal to correct the record and the reason for the refusal, that the record has been annotated, and that the applicant may ask for a review of the refusal under Part V.

Under the *ATIPP Act*, individuals have the right to make a complaint to the Government of Newfoundland and Labrador's Information and Privacy Commissioner about the refusal to correct the record of personal information.

5.7 Protection of Personal Information

36 *The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.*

Section 36 requires the head of a public body to ensure there are reasonable security measures to protect personal information in the custody or under the control of the public body. Security measures can include physical, administrative and technical safeguards.

“Reasonable” security arrangements should take into account the sensitivity of the information being protected, the potential harm of unauthorized access, and the medium in which the information is transferred, transmitted or stored.

5.7.1 Physical safeguards

Physical safeguards monitor and control the work environment. Examples of physical safeguards include:

- *storing personal information in locked filing cabinets, offices and buildings, with controls over distribution of keys or lock combinations*
- *storing personal information in secure areas where access is limited or restricted*
- *logging out of [or locking] computers when stepping away from the work area*
- *not leaving documents containing personal information on printers or fax machines*
- *shredding any documents containing personal information prior to disposal*
- *labeling files containing personal information as a reminder to store them securely*
- *card access systems, video surveillance and security guards*

5.7.2 Administrative safeguards

Administrative controls provide a framework for operating and managing the work environment, and should be formalized in written policies and procedures. Key policies related to privacy should cover Security, Records Management, Information Management, and the definition of administrative ‘Roles and Responsibilities’. Examples of administrative safeguards include policies, procedures and practices that:

- *Ensure organized and secure management of records containing personal information;*
- *Limit access to records containing personal information to authorized employees and agents who need to know this information to carry out their duties;*
- *train employees on privacy, safeguards and security of personal information;*
- *incorporate file check-out procedures for records containing personal information;*
- *outline procedures to identify ‘sensitive’ personal information and ensure secure transfer and use of that information (e.g. only faxing sensitive personal information in a manner than ensures it will be received by the intended recipient);*
- *manage and audit employee access to records containing personal information; and*
- *verify an individual's identity when requesting personal information.*

5.7.3 Security and technical safeguards

Technical or “logical” safeguards monitor and control access to information and computer systems. Examples of technical safeguards include:

- *Role-based access controls and strong password protection to determine user authentication and authorization*
- *Audit features and access logs to track system access and use*
- *data encryption of personal information during file transfers*
- *data encryption of personal information stored on laptops & removable media devices*
- *back up of files containing personal information*
- *Network security protection and monitoring (e.g. firewalls, network intrusion detection)*

5.8 Retention of Personal Information

37 *Where a public body uses an individual's personal information to make a decision that directly affects the individual, the public body shall retain that information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it.*

By requiring public bodies to keep personal information for at least a year, individuals are given a reasonable opportunity to access their personal information, and request corrections, where applicable. Please note the year runs from the date the information was used to make a decision about the individual.

If an individual's personal information is used to make a decision, public bodies should place a note on file indicating the:

- *Details of the decision; and*
- *Date the decision was made.*

If a public body does not use the personal information to make a decision directly affecting the individual, the Act does not require the personal information to be retained. For example:

A public body uses personal client information to study trends and program effectiveness within a target demographic and does not subsequently use that information to make a decision about an individual. The retention requirements of section 37 do not apply in this situation.

A public body uses personal client information to determine if an applicant is entitled to a grant. The retention requirements of section 37 do apply in this situation.

Disposal of records containing personal information should occur in accordance with approved records retention and disposal schedules. For additional information related to the management and disposal of Government records, see the *Management of Information Act* and *The Rooms Act* at the House of Assembly website:

Management of Information Act

<http://www.hoa.gov.nl.ca/hoa/statutes/m01-01.htm>

The Rooms Act

<http://www.hoa.gov.nl.ca/hoa/statutes/r15-1.htm>

5.9 Use of Personal Information

Section 38 stipulates the circumstances where public bodies may use personal information.

38 (1) *A public body may use personal information only*

- (a) *for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose as described in section 40;*
 - (b) *where the individual the information is about has identified the information and has consented to the use, in the manner set by the minister responsible for this Act; or*
 - (c) *for a purpose for which that information may be disclosed to that public body under sections 39 to 42.*
- (2) *The use of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is used.*

Any use of personal information that does not meet the above criteria is not permissible under the *ATIPP Act*. It is important to examine this section if you intend to use personal information for a use other than the originally intended purpose.

Section 38 allows information to be used for certain purposes other than the original purpose of the collection. If a public body is allowed under section 38 to use personal information for another purpose, they should document the new use and cite the clause(s) of the *ATIPP Act* that allows them to use this information for a new purpose. This should be done even in instances where the public body believes that the new use is consistent with the purpose for which the personal information was originally collected.

5.9.1 Use for original purpose or consistent purpose

A public body may use personal information for the purposes for which it was originally collected or compiled. The purpose of the collection must be authorized under section 32 ([“Purpose for which personal information may be collected”](#)).

The *ATIPP Act* also allows personal information to be used for a “consistent purpose”, which is defined in section 40 as:

40. *A use of personal information is consistent under section 38 or 39 with the purposes for which the information was obtained or compiled where the use:*
- (a) *has a reasonable or direct connection to that purpose; and*
 - (b) *is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.*

There are no hard and fast rules as to what constitutes a use for a consistent purpose. One guideline to consider is whether a reasonable person would anticipate or expect the personal information to be used in the newly proposed way, even if this use was not spelled out at the time the personal information was originally collected. If you are unsure if a purpose can be considered a ‘consistent purpose’, please consult your Department’s solicitor.

5.9.2 Individual has identified the information & consented to its use

Any consent by an individual to a proposed new use must be an informed consent. The individual should be informed of:

- *the nature of personal information held by the public body about the individual which is proposed to be used;*
- *the proposed **new** use for the personal information; and*
- *the potential impact or consequences on the individual of his or her consent to the new use for the personal information.*

If additional uses are anticipated at the time of collection, consent for the additional use should be obtained at that time. Consent may, however, be requested later, if the new use is not proposed until after the original collection. For example:

A public body compiles a mailing list containing names and home addresses for one of its programs. It then begins a new program and plans to use the same mailing list for this program. If the programs are unrelated this use of the personal information is not consistent with the use for which the public body originally collected it, and the public body must get consent from each individual before including her or his personal information on the second mailing list.

The classes of persons who may provide consent for minors, incompetents, deceased persons, or other individuals in giving or withholding consent are contained in *section 65* of the *ATIPP Act*.

5.9.3 Use consistent with sections 39-42

Public bodies are permitted to use personal information that may be disclosed under *sections 39 to 42*. These sections set out the circumstances where public bodies may disclose personal information. Examples of disclosure under this section include information disclosed:

- *for statistical purposes (s. 41)*
- *for archival purposes (s. 42)*
- *to the Auditor General (s. 39(1)(j)).*

Section 33(1)(b) allows public bodies to use the information disclosed in accordance with these sections. For a detailed description of the disclosure requirements within the *ATIPP Act*, see [section 5.10 Disclosure of Personal Information](#).

5.9.4 Minimum amount of information to be used

Public bodies are required to ensure their use of personal information is limited to the minimum amount of information necessary to accomplish the purpose for which it is used. This means, as well, that access to and use of personal information by employees or agents of the public body must be limited to those who need to know the information to carry out the purpose for which the information was collected or to carry out a purpose authorized under *section 38*.

5.10 Disclosure of Personal Information

Section 39 lists the circumstances under which public bodies may disclose personal information:

- 39 (1) *A public body may disclose personal information only*
- (a) *in accordance with Parts II and III;*
 - (b) *where the individual the information is about has identified the information and consented to the disclosure in the manner set by the minister responsible for this Act;*
 - (c) *for the purpose for which it was obtained or compiled or for a use consistent with that purpose as described in section 40 ;*
 - (d) *for the purpose of complying with an Act or regulation of, or with a treaty, arrangement or agreement made under an Act or regulation of the province or Canada ;*
 - (e) *for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information;*
 - (f) *to an officer or employee of the public body or to a minister, where the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer, employee or minister;*
 - (g) *to the Attorney General for use in civil proceedings involving the government;*
 - (h) *for the purpose of enforcing a legal right the government of the province or a public body has against a person;*
 - (i) *for the purpose of*
 - i) *collecting a debt or fine owing by the individual the information is about to the government of the province or to a public body, or*
 - ii) *making a payment owing by the government of the province or by a public body to the individual the information is about;*
 - (j) *to the Auditor General or another person or body prescribed in the regulations for audit purposes;*
 - (k) *to a member of the House of Assembly who has been requested by the individual the information is about to assist in resolving a problem;*
 - (l) *to a representative of a bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry;*
 - (m) *to the Provincial Archives of Newfoundland and Labrador , or the archives of a public body, for archival purposes;*
 - (n) *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, or*
 - ii) *from which a law enforcement proceeding is likely to result;*
 - (o) *where the public body is a law enforcement agency and the information is disclosed*
 - i) *to another law enforcement agency in Canada , or*
 - ii) *to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority;*
 - (p) *where the head of the public body determines that compelling circumstances exist that affect a person's health or safety and where notice of disclosure is mailed to the last known address of the individual the information is about;*

-
- (q) *so that the next of kin or a friend of an injured, ill or deceased individual may be contacted;*
 - (r) *in accordance with an Act of the province or Canada that authorizes or requires the disclosure; or*
 - (s) *in accordance with sections 41 and 42 .*

39 (2) *The disclosure of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.*

If a disclosure cannot be justified by this section, the personal information should not be disclosed. Please note that the term ‘**disclosure**’ includes a disclosure to another public body. A public body includes another government department, a government agency, a post secondary institution, health boards, school boards and municipalities.

On occasion, personal information may be accidentally disclosed in contravention of the privacy provisions in the *ATIPP Act*. This is referred to as a “**privacy breach**”. For information about breaches of personal information, see section [5.12 Privacy Breaches](#).

5.10.1 Discretion to disclose

39 (1): *A public body may disclose personal information only....*

As indicated by the word ‘**may**’, *section 39* does not require disclosure. Rather, it permits disclosure at the discretion of the public body.

If a public body determines it has authority to release personal information, it must determine whether to exercise its discretion to disclose. The public body should consider if it is appropriate to disclose the information in that circumstance, taking into account both the potential harm that could result from disclosure (including the harm to an individual's privacy) and the consequences of not disclosing the information.

The following is a summary of some of the general principles that apply to the exercise of discretion:

“... the discretion must be exercised by the authority to which it is committed, which must act on its own and not under the dictation of any other body, and ... it must be willing to exercise its discretion in each individual case which comes before it. The authority must act in good faith, must have regard to all relevant considerations and must not be swayed by irrelevant considerations, must not seek to promote purposes alien to the letter or to the spirit of the legislation which gives it power to act, and must not act arbitrarily or capriciously.”¹

In some cases, other authorities may require disclosure. For example:

- *disclosure may be required by an Act of the province or Canada, or*
- *disclosure may required in response to a subpoena, warrant or other order of a court or tribunal*

¹ *Administrative Law* by Evans, Janisch, Mullan and Risk (1980), at page 623.

5.10.2 Minimum amount of information to be disclosed

39 (2): The disclosure of personal information by a public body shall be limited to the minimum amount of information necessary to accomplish the purpose for which it is disclosed.

Under this section, only a minimum amount of information should be disclosed. For example, in responding to a subpoena, warrant or other order, the public body should provide only the personal information specifically requested in the subpoena, warrant or order. Where the subpoena, warrant or order is unclear, public bodies should consult their legal counsel. For example, if a public body receives a court order to release a person's address to law enforcement officials, the public body should not release the person's telephone number or health status.

5.10.3 Request for disclosure

Unless compelling reasons exist requiring the contrary, disclosures should be recorded in writing. If a public body receives a verbal request for personal information and discloses it verbally, the conversation should be recorded in writing. This ensures that if there is a future dispute about a disclosure, there is a written record of what happened.

Public bodies should ensure any requests for personal information comply with the *ATIPP Act*. They should generally contain the following details:

- *the name of the individual whose information is requested*
- *the nature of the information desired*
- *the authority for the disclosure*
- *the purpose for which the requestor(s) will use the information, and*
- *the name, title and address of the person authorized to make the request*

However, there may be some circumstances where not all this information is available, and public bodies should use their discretion to determine whether the request contains sufficient information. For example, some details may not be available if the information is being requested in an emergency.

The written request for personal information under this section and the outgoing correspondence (recording the fact that disclosure did or did not take place) should be retained on file. A written record of a verbal request and disclosure should be retained on file.

5.10.4 Consent to disclosure from the individual

39 (1) A public body may disclose personal information only

(b) Where the individual the information is about has identified the information and consented to the disclosure in the manner set by the minister responsible for this Act.

A public body is permitted to disclose personal information if the individual the information is about consents to the disclosure. Consent should be clear and specific, and the public body should be satisfied that:

- *the consent is voluntary and;*
- *the consent is "informed", that is, the individual understands the effects and consequences of the consent.*

Where possible, an individual's consent should be in writing. If consent is given verbally, the public body should make a written record of the conversation and, where reasonable, send a letter to the individual confirming the consent.

The individual's consent should include:

- *a description of the personal information to be disclosed*
- *the purpose of the disclosure*
- *the recipient(s) of the disclosed personal information*
- *the date of the consent and the period of time during which the consent remains valid*
- *the public body to which the consent is being given*

Consent to disclose should be sought at the time the personal information is collected, where the disclosure is anticipated. Where the disclosure is not anticipated, consent may be obtained at a subsequent time, provided it is obtained before the proposed disclosure.

In limited circumstances, consent to disclose personal information for the purposes of *section 39(1)(b)* may be provided by certain persons on behalf of the individual the information is about, under *section 65* of the *ATIPP Act* “**Exercising rights of another person**”.

5.10.4.1 Disclosure for consistent purpose

40. A use of personal information is consistent under section 38 or 39 with the purposes for which the information was obtained or compiled where the use

(a) has a reasonable and direct connection to that purpose; and

(b) is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information.

Sections 38 and 39, state that uses or disclosures are permissible if they are consistent with the original purpose for which the personal information was collected. *Section 40* states criteria by which a use of personal information is deemed consistent with the use that is was obtained or compiled under *sections 38 and 39*:

Public bodies should determine if the use of the personal information:

- *has a reasonable and direct connection to the purpose for which it was obtained or compiled; and*
- *is necessary for performing the statutory duties of, or for operating a legally authorized program of, the public body that uses or discloses the information*

If it cannot be determined that both criteria listed above have been met, the use must be justified under *section 38(1)(b) or (c)*. This will often mean seeking the consent of the individual the information is about before proceeding with the intended use or disclosure.

5.10.5 Disclosure for Research or Statistical Purposes

A public body may release personal information to assist with research. This need arises when the nature of the research itself, or the records involved, makes it unfeasible to conduct the research without information that identifies individuals.

Section 41 permits [but does not require] a public body to disclose personal information for purposes related to research, providing four conditions have been met:

- 41 *A public body may disclose personal information for a research purpose, including statistical research, only where*
- (a) *the research purpose cannot reasonably be accomplished unless that information is provided in individually identifiable form;*
 - (b) *any record linkage is not harmful to the individuals that information is about and the benefits to be derived from the record linkage are clearly in the public interest;*
 - (c) *the head of the public body concerned has approved conditions relating to the following:*
 - i) *security and confidentiality,*
 - ii) *the removal or destruction of individual identifiers at the earliest reasonable time, and*
 - iii) *the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of the public body; and*
 - (d) *the person to whom that information is disclosed has signed an agreement to comply with the approved conditions, this Act and the public body's policies and procedures relating to the confidentiality of personal information.*

The public body has the final responsibility in administering and approving research agreements. Before releasing any information, there should be a written agreement between the public body and the researcher. The public body should be satisfied that:

- *Access privileges are only used for the purpose stated in the agreement, and are not used as a means to browse records.*
- *The researcher will not disclose or share personal information with any other party, except as set out in the agreement*
- *The researcher will destroy any personal identifiers as soon as possible*
- *The researcher will not use personal information for any purpose other than the purpose set out in the agreement*
- *There are appropriate security measures in place to protect personal information*

The public body should confirm and document that the applicant requires access to records containing personal information in individually identifiable form in order to achieve the research purpose. The personal information must be directly related to the research - this may occur where the applicant needs to see the information in personally identifiable form for their research but does not need to provide the results or analysis of their research in a personally identifiable form.

The researcher must sign a detailed research agreement that describes the nature of the research, type of personal information that will be disclosed, how it will be used, any terms and conditions for the disclosure, and the procedural safeguards that the researcher will use for its protection. Only the researcher, or an authorized agent of the researcher, may sign a research agreement. Research agreements should not be ongoing or "open-ended" but may be renewed, as required.

5.10.6 Disclosure for Archival or Historical Purposes

Section 42 states the circumstances under which the Provincial Archives of Newfoundland and Labrador or the archives of a public body may disclose personal information.

- 42 *The Provincial Archives of Newfoundland and Labrador, or the archives of a public body, may disclose personal information for archival or historical purposes where*
- (a) *the disclosure would not be prohibited by section 30;*
 - (b) *the disclosure is for historical research and is in accordance with section 41;*
 - (c) *the information is about an individual who has been dead for 20 years or more; or*
 - (d) *the information is in a record that has been in existence for 50 years or more.*

This section recognizes the unique challenges faced by the Provincial Archives or the archives of a public body in complying with both the access and privacy components of the *ATIPP Act*. Archives have legal custody of enormous volumes of records to which the public has a right of access. Many of these records contain very sensitive personal information. *Section 42* provides four circumstances under which an archive may legally disclose personal information at its discretion. Archives are not obliged to disclose personal information under this section.

5.10.7 Disclosure to a Member of the House of Assembly

Section 39(1)(k) permits disclosure of personal information to a Member of the House of Assembly (MHA) who has been requested by the individual the information is about to assist in resolving a problem. An MHA is a person elected as a representative of a constituency within the province of Newfoundland and Labrador to represent the interests of the voters in that constituency in the House of Assembly.

This provision permits disclosure only to MHAs of Newfoundland and Labrador, and only to assist the person concerned to resolve a problem. In practice, MHAs may designate their constituency assistants to act on their behalf in requesting personal information under section 39(1)(k). MHAs should be asked to provide a list of designated staff to public bodies so that public bodies know who is authorized to act on the MHA's behalf.

The provision does not permit the disclosure of personal information to federal Members of Parliament or municipal representatives. These representatives may, however, obtain personal information about an individual with his or her consent.

The purpose of disclosure under section 39(1)(k) must be to assist in resolving a problem. This includes helping an individual to provide information to a public body, inquiring about decisions or about a service or benefit, or correcting a mistake or misunderstanding.

A public body employee who receives this type of request from an MHA may inquire about the purpose of the request in order to confirm that the disclosure is necessary to assist in resolving a problem. **It is important to note that verbal consent made to the MHA is sufficient for disclosure under section 39(1)(k).** Although not required by the *ATIPP Act*, it is suggested that MHAs obtain written consent where practical. If written consent cannot be obtained, some record (e.g. an annotation to file) should be kept for verbal requests and/or consent given. The inquiry and disclosure should be recorded in writing by the public body. Where inquiries and disclosure take place verbally, the transaction should be noted on the affected person's file. The ATIPP Office has developed a form that can be used by MHAs to annotate verbal consent and which can be filed by the public bodies to document requests.

5.11 Privacy Tools for Assessing Compliance

The ATIPP Office has developed a number of tools to help public bodies assess compliance with the privacy provisions of the *ATIPP Act*. These tools, while based on legislative compliance, also incorporate the 10 privacy principles, discussed in section [5.1 Fair Information Practices](#).

The following tools are used to assess compliance with the *ATIPP Act*:

Annual Privacy Checklist

- *Used to determine a public body's compliance, from a broad perspective*
- *Used to assess privacy risks*
- *Can be completed quickly and without privacy expertise*
- *Should be completed every year*

Privacy Impact Assessment (PIA) Protocol

The *PIA Protocol* is a framework to assess the compliance of a project, and contains two tools:

1) Preliminary PIA Checklist

- *Used to assess if a PIA should be completed for a project*
- *Should be done on all new projects/systems and extensive project upgrades*
- *Can be completed quickly and without privacy expertise*

2) Privacy Impact Assessment (PIA)

- *Used to ensure privacy issues are fully considered at an early stage of project development, particularly where there are significant privacy risks*
- *Completed for projects where the Preliminary PIA has indicated a PIA is necessary*
- *Requires a team which includes members who have significant privacy expertise, technical expertise, and knowledge about the project*

5.11.1 Annual Privacy Checklist

The **Annual Privacy Checklist** is a tool used to assess departmental compliance with the *ATIPP Act*. The Checklist contains questions on privacy issues that examine how public bodies collect, use, disclose, exchange and retain personal information. Questions can usually be answered with a simple checkmark, but additional details are often helpful when assessing the Checklist.

The Checklist is a Microsoft Excel-based form and is available from the ATIPP Office. To view a paper version of this checklist tool, see [Appendix C: Annual Privacy Checklist](#).

You should contact your Senior Privacy Analyst in the ATIPP Office if you have questions or need assistance completing the Checklist. When the electronic version of the Checklist is completed, it should be forwarded by email to your Senior Privacy Analyst. Please contact the ATIPP Office for a full listing of Senior Privacy Analysts.

5.11.1.1 Checklist questions

The Checklist covers a variety of topics about the collection, use and disclosure of personal information. The topics include:

- *Exchange of personal information between Departments and external to Government*
- *Physical, Administrative and Technical Safeguards*
- *Kinds of personal information being collected, used and disclosed*
- *Authorization for collections of personal information*
- *Method of collecting personal information*
- *Retention and retrieval of personal information*
- *Training and formal instructions to staff dealing with personal information*

The Annual Privacy Checklist is designed so that it can be completed without privacy expertise, though you may find basic privacy training useful prior to completion.

5.11.1.2 How many checklists should be completed?

A Checklist should be completed for **at least** every division of your Department. However, many divisions provide a variety of different programs that collect personal information. There may be significant differences in how these programs collect, use and disclose personal information. Unless personal information is handled in the same way for each program, a Checklist should be completed for **every** program.

Before deciding how many Checklists your Department should complete, it may be helpful to review the Checklist to see what kinds of questions will be asked, and whether the answers will require you to distinguish between programs.

5.11.1.3 Who should complete the checklist?

The Checklist should be completed by the Director of the division. The Director can delegate this task to another staff member, but the person who completes the Checklist should be familiar with the Department's policies, procedures and practices.

5.11.1.4 What if a division does not collect personal information?

In rare cases, a Division may not collect, use or disclose personal information. If this is the case, you should complete the **Declaration of No Personal Information** section, which appears at the end of the Checklist.

You should be very cautious when stating you do not collect personal information. If you believe this is the case, you should review the definition of personal information contained in the ATIPP Act, *section 2(o)*.

5.11.1.5 How long will it take to complete the Checklist?

The time it takes to complete the Checklist will vary, depending on the volume of personal information involved and the complexity of the operational environment. However, the amount of time required will usually not exceed 2 hours.

5.11.1.6 Checklist results and scoring

Completed checklists are scored on a “traffic light” system (red, yellow or green), as well as a calculated numerical score. The score will indicate the level of compliance with the privacy provisions of the *ATIPP Act*:

- Green** *Overall ATIPP compliance is good, although there may be specific areas that need to be addressed.*
- Yellow** *Mitigating factors do not compensate for ATIPP risks identified. Consult with your Senior Privacy Analyst in the ATIPP Office.*
- Red** *High risk of ATIPP non-compliance. IMMEDIATE ACTION REQUIRED.*

Checklist scores can be viewed by clicking the “Scores” tab at the bottom of Checklist.

Even if a Division scores in the green, there are usually opportunities to improve compliance further. If you receive a red score, you should consult your Senior Privacy Analyst in the ATIPP Office to discuss your answers and mitigate possible privacy concerns. In many cases, simple steps can quickly improve a low score and improve overall levels of privacy compliance.

5.11.1.7 Submitting Checklists to the ATIPP Office

Once the Checklist is complete, forward it to your Senior Privacy Analyst in the ATIPP Office. The Analyst will review the Checklist and may contact you with questions about your answers.

5.11.1.8 Checklist follow-up

When all Checklists have been received from your Department, your Senior Privacy Analyst in the ATIPP Office will meet with representatives of the Department, usually including the ATIPP Coordinator for your Department, to develop a **Privacy Plan**.

In developing the Privacy Plan, your Senior Privacy Analyst in the ATIPP Office will work with your Department to identify actions to be taken to improve privacy compliance. The completed Privacy Plan will identify strategies, appropriate timelines, and the individuals responsible for ensuring those tasks are completed. Once the Privacy Plan is completed, the Analyst will meet with your Department on a regular basis to monitor progress of completion.

5.11.2 Privacy Impact Assessment (PIA) Protocol

A **Privacy Impact Assessment (PIA)** is a formal evaluation of the privacy implications within a specific project. The term "project", in this context, is very broad; it refers to a project, program, initiative, legislation, system, application, program, or any other defined course of endeavor.

The Government of Newfoundland and Labrador's *PIA Policy* states:

"Public Bodies within the Government of Newfoundland and Labrador will conduct PIAs for all new and significantly redesigned collections, uses or disclosures of Personal Information that may raise potential privacy risks."

To view the full *PIA Policy*, see [Appendix D: PIA Policy](#).

The PIA Protocol is a joint framework implemented by the ATIPP Office and the Office of the Chief Information Officer (OCIO) that will assess privacy concerns and identify privacy mitigation strategies for IT-led projects.

Projects that are not IT-related will follow a condensed version of the PIA Protocol that excludes OCIO involvement.

The purpose of the PIA Protocol is to:

- Identify potential areas of non-compliance with the ATIPP Act
- Identify risks associated with privacy compliance
- Identify measures to mitigate privacy risks
- Assess compliance with the *Fair Information Practices* (discussed in section 5.1.1)

5.11.2.1 Stages of the PIA Protocol

The stages of the PIA Protocol include:

1. Identify Project
2. Complete Preliminary PIA
3. Evaluate Preliminary PIA
4. Initiate PIA
5. Conduct PIA
6. Review PIA
7. Obtain Sign Off

To see an overview of the PIA Protocol and its stages, see [Appendix E: PIA Protocol](#).

Stage 1: Identify Project

The first step of the PIA Protocol is to identify the project. Because all new projects must go through this process, Departments and Project Managers should remember to consider privacy issues at an early stage in the Project Management lifecycle.

Who is responsible for identifying the project?

For IT-led projects, the OCIO will alert the ATIPP Office of projects that require an analysis of privacy issues. Project Managers are required to initiate a privacy discussion with the OCIO's Information Protection Analyst in order to assess privacy concerns within their projects.

Projects may also be identified by a Department, Project Sponsor or the ATIPP Office.

When should a project be assessed for privacy concerns?

Ideally, Project Managers should start addressing privacy assessment early in the planning process, after the project has received formal authority to proceed and prior to the development phase of the project. Early privacy awareness allows stakeholders to identify privacy issues during the planning phase and possibly avoid costly redesigns during and after project development.

If a project uses little or no personal information, do I still need to follow the PIA Protocol?

The PIA Protocol should be implemented for all new and significantly redesigned projects. Even if you think a project carries few privacy risks, **it is mandatory to complete the Preliminary PIA for all projects.** If the Preliminary PIA indicates that there are few or no privacy risks associated with the project, you will not spend valuable time and resources completing a more comprehensive evaluation of privacy with a PIA.

Stage 2: Complete Preliminary PIA

It is mandatory that Project Managers complete a Preliminary PIA for their projects. The Preliminary PIA is a tool used to assess whether a more comprehensive evaluation of privacy, such as a PIA, is required for a specific project. It contains questions about the privacy and security measures involved in a project. Like the Annual Privacy Checklist, it is designed to be completed by people with little or no privacy expertise.

The Preliminary PIA consists of questions that identify the collection, use and disclosure of personal information within the project and assess possible privacy risks that may require additional privacy planning in the form of a PIA. The Preliminary PIA will include topics such as:

- Project description and costs
- Completion of previous PIAs
- Departments involved in the project
- Collection, use and disclosure of personal information
- Information security and safeguards

To view a paper version of the Preliminary PIA project checklist, see [Appendix F: Preliminary PIA](#).

Who should complete the Preliminary PIA?

The Preliminary PIA should be completed by the Project Manager, who has the primary operational responsibility for the project. However, the Project Manager may seek assistance from other parties, such as your Senior Privacy Analyst in the ATIPP Office and the Information Protection Analyst in the OCIO. On occasion, the Preliminary PIA may be completed by the Project Sponsor or another individual who is designated as the primary resource for the project.

If I know a project will involve significant amounts of personal information and there are significant privacy risks, do I need to conduct a Preliminary PIA or can I go straight to the PIA?

Even if the need for a PIA is evident, Preliminary PIAs are mandatory for all projects. Even where it is known that a PIA will be required, the Preliminary PIA is a useful first step in identifying privacy issues in the project.

How do I submit a Preliminary PIA for evaluation?

For IT-led projects, the Project Manager will submit the completed Preliminary PIA by email to the Department's Senior Privacy Analyst in the ATIPP Office and Information Protection Analyst in the OCIO. For projects that are not IT-related, the Preliminary PIA will be submitted by email to the Department's Senior Privacy Analyst in the ATIPP Office.

Stage 3: Evaluate Preliminary PIA

For IT-led projects, the Preliminary PIA will be reviewed by your Senior Privacy Analyst in the ATIPP Office and the Information Protection Analyst in the OCIO. The evaluation process will involve a review of the Preliminary PIA content and may require several discussions or meetings with the Project Manager and/or other key individuals working with the project. Upon completion of the evaluation process, the ATIPP Office and OCIO will issue a joint **Recommendation Letter** indicating whether a full PIA should be conducted for the project.

For projects that are not IT-related, the Preliminary PIA will be reviewed by your Senior Privacy Analyst in the ATIPP Office and a Recommendation Letter will be issued by the ATIPP Office.

Who makes the decision to proceed with a PIA?

Since Departments are ultimately responsible for privacy compliance, the decision to proceed or not proceed with a PIA after a recommendation has been made must lie with the responsible Department(s) involved in the project, including the OCIO in cases of joint IT-led projects.

Stage 4: Initiate PIA

When the decision has been made to proceed with a PIA, the Project Manager, in consultation with the ATIPP Office and, for IT-led projects, the OCIO, is responsible for the formation of the PIA Team. The PIA Team will meet to discuss the project, timelines, outsourcing and an approach for completion of the PIA, which may include assigning tasks to specific team members, as required.

How is a decision made to outsource a PIA?

Wherever possible, PIAs will be completed in-house within the Government of Newfoundland and Labrador. Any decision to outsource a PIA will be made collectively by the OCIO, ATIPP Office, and client Department, on a case-by-case basis, depending on the needs of the project.

Who will participate in the PIA Team?

The PIA Team will include subject matter experts on privacy and security, as well as individuals with knowledge of the project and departmental operations, including (but not limited to):

Project Manager

The Project Manager is the person with primary operational responsibility for ensuring that the project is brought to a successful conclusion. The Project Manager, in consultation with other PIA Team members, is responsible for ensuring the PIA Protocol is followed and the PIA is completed for the project. If the project does not have a Project Manager assigned, the manager who otherwise carries day-to-day responsibility for the Project is responsible for conducting the PIA.

ATIPP Office

The ATIPP Office, in cooperation with the OCIO, is responsible for developing and maintaining the PIA Protocol. The ATIPP Office will provide advice on privacy issues and assist Departments in completing privacy checklists and PIAs. The ATIPP Office is also responsible for ensuring that privacy tools, the PIA Protocol and its procedures are understood throughout the Government of Newfoundland and Labrador. Your Senior Privacy Analyst in the ATIPP Office will provide privacy expertise and guidance throughout the entire PIA process.

OCIO

The OCIO, in consultation with Departments and the ATIPP Office, is responsible for the review and approval of PIAs for IT-led projects. The OCIO is also responsible for ensuring that security Threat and Risk Assessments (TRA) are undertaken as necessary to ensure appropriate security measures for the project, as stated in section 36 of the *ATIPP Act*.

The OCIO will take the lead in addressing the technical components of privacy issues and, in cooperation with the ATIPP Office, will incorporate the PIA Protocol and procedures into its Project Management standards. For IT-led projects, the CIO of the Government of Newfoundland and Labrador will be required to review, approve and sign-off on the completed PIA.

Department Head

The Department Head is responsible for compliance with the privacy provisions of the *ATIPP Act*, including the responsibility for ensuring that PIAs are completed in accordance with the PIA Protocol and PIA Policy. Departmental representatives delegated by the Department Head will participate in the PIA Team. If the project is a joint initiative between several Departments, all these Departments should be involved in the PIA process.

The Department Head, or an individual delegated in writing by the Department Head, will be required to review, approve and sign-off on the completed PIA. When completed, the PIA shall be reviewed and approved by the Department Head, or by a person delegated in writing by him or her to review and approve PIAs.

Other PIA Team Members

Depending on the project, the team may want to engage other experts with varying levels of expertise to participate in the PIA Team and assist with the completion of the PIA, including Project staff. For example, the team may need to assistance of the Department's Solicitor to clarify legal issues. The team may also involve other key individuals or stakeholders involved in the project, as required.

For additional information about stakeholder 'Roles and Responsibilities' when completing a PIA, see [Appendix D: PIA Policy](#).

Stage 5: Conduct the PIA

When a decision is made to complete the PIA within government (i.e. the PIA is not outsourced to an external vendor), the PIA Team will begin completion of the PIA Template, a compliance-based tool created by the ATIPP Office in consultation with the OCIO.

The PIA Template contains the following sections:

1. Basic Information
2. Department Information
3. Project Description
4. Security and Safeguards
5. Collection of Personal Information
6. Use of Personal Information
7. Disclosure of Personal Information
8. Accuracy, Correction and Retention of Personal Information
9. Privacy Risks and Risk Mitigation Strategies
10. PIA Team Review
11. Authorization and Approval

While some of the questions require only yes/no answers, others require more complete explanations. Some questions will require you to attach policies and other detailed descriptions in a separate document.

The section of the PIA entitled “*Privacy Risks and Risk Mitigation Strategies*” is very important in that it will identify those areas of the project with privacy concerns. This section will require the PIA Team to propose mitigation strategies in order to limit privacy risks in the project.

The PIA Team should review the questions in detail and discuss how each team member can assist with the process of completing the PIA. While the Project Manager is responsible for ensuring completion of the PIA, it may be appropriate to assign tasks to various team members, as required.

The Annotated Template contains additional information about how to complete the PIA, including explanations of the questions. The annotated template is given for information purposes - the PIA itself should be completed in the non-annotated electronic version, available from the ATIPP Office.

To view the annotated version of the PIA Template, see [Appendix G: PIA Template \(Annotated\)](#)

Stage 6: Review PIA

After the PIA Template has been completed and all supporting documentation has been compiled, the PIA team will review the entire PIA and risk mitigation strategies.

Upon review, a final draft of the PIA will be distributed to all team members for their approval. All team members must review the final version of the PIA and this review will be noted in *Section 9*, “**PIA Team Review**”. This section will also allow PIA team members to address any concerns they may have with the proposed risk mitigation strategies recommended in the PIA.

Stage 7: Obtain Sign-off

The final section of the PIA template, “**Authorization and Approval**”, requires sign off from the following individuals:

- Project Manager
- OCIO Director (responsible for the Project Manager)
- Deputy Minister
- Chief Information Officer (for IT-led projects only)

Prior to seeking the signatures for sign-off, the final version of the document should be circulated to ensure each party is satisfied with the final version. If more than one Department is involved, the Deputy Minister of each department should sign off on the completed PIA.

Your Senior Privacy Analyst in the ATIPP Office can assist the Project Manager with the communication aspects of acquiring signatures for final PIA approval.

5.12 Privacy Breaches

Public bodies should make every effort to prevent privacy breaches from occurring. They should also be aware of the steps to be taken when a breach occurs. For a summary of the steps involved in responding to a privacy breach, please see [Appendix H: Privacy Breach Protocol](#).

5.12.1 What is a privacy breach?

A privacy breach occurs when there is unauthorized collection, use, disclosure or disposal of personal information. Such activity is “unauthorized” if it occurs in contravention to the *ATIPP Act*. The most common privacy breach happens when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed. For example, a privacy breach occurs when a computer containing personal information is stolen or when personal information is mistakenly emailed to the wrong person.

5.12.2 Consequences of a privacy breach

Privacy Breaches can cause significant harm to individuals, including:

- *Identity theft*
- *Safety being compromised*
- *embarrassment about their personal information being disclosed*

There are also consequences for the public body and its employees, including

- *The Privacy Commissioner may commence an investigation into the incident*
- *The Department may be obliged to devote time & resources to correction of the breach*
- *The Department may suffer damage to its reputation as a result of the breach*
- *If a breach is intentional, a fine of up to \$5,000.00 and/or a jail term of up to six months*
- *The Privacy Act also gives individuals the right to sue the Government of Newfoundland and Labrador for invasion of privacy*

5.12.3 Examples of a privacy breach

In 2004, the government of Alberta outsourced management of vehicle registries to a private company. In November of that year, prison guards asked the province to remove their home addresses from the automobile registries. At least six prison guards had received threats from gang members. One guard was told by a gang member that the registry databases had been infiltrated by insiders.¹

In July 2005, the British Columbia Ministry of Labour sold a set of high-capacity data tapes to a surplus computer equipment store. The tapes were purchased at a public auction for \$101. The buyer turned the tapes over to a newspaper after realizing the tapes contained health and immigration records, including information on sexual abuse, HIV status and mental illness.²

¹ “Prison Guards Protest Privacy Breach,” website: www.cbc.ca, November 15, 2004, www.cbc.ca/canada/edmonton/story/2004/11/15/ed_prisonguards20051115.html

² “Health and Immigration Records Sold at B.C. Auction,” website: www.cbc.ca, March 6, 2006, www.cbc.ca/canada/story/2006/03/06/bc-government-tapes060306.html

5.12.4 Four key steps in responding to a privacy breach

The most important step you can take is to respond immediately to the breach. You should undertake steps 1, 2 and 3 below immediately following the breach and do so simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies.

5.12.4.1 Step 1: Contain the breach

You should take immediate common sense steps to limit the breach:

- *Immediately contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached or correcting weaknesses in physical security.*
- *Immediately contact your Director/Manager, your Privacy Analyst, and/or the person responsible for security in your organization.*
- *Immediately retrieve the Privacy Breach Reporting Form, located at Appendix 13. When the form is complete, submit it to your Senior Privacy Analyst in the ATIPP Office*
- *Work with your privacy/management team to provide appropriate notification as outlined in the Privacy Notification Assessment Tool, located at Appendix 14.*

5.12.4.2 Step 2: Evaluate the risks associated with the breach

To determine what other steps are immediately necessary, you should assess the risks associated with the breach. Consider the following factors in assessing the risks:

1) Personal information involved

- a) What data elements have been breached? In many cases, the risk of harm increases with an increase in the sensitivity of data. Health information, social insurance numbers and financial information that could be used for identity theft are examples of sensitive personal information.
- b) Can the information be used for fraudulent or otherwise harmful purposes?

2) Cause and extent of the breach

- a) What is the cause of the breach?
- b) Is there a risk of ongoing or further exposure of the information?
- c) What was the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including in mass media or online?
- d) Is the information encrypted or otherwise not readily accessible?
- e) What steps have you already taken to minimize the harm?

3) Individuals affected by the breach

- a) How many individuals are affected by the breach?
- b) Who was affected by the breach: employees, public, contractors, clients, service providers, other organizations?

4) Foreseeable harm from the breach

- a) Is there any relationship between the unauthorized recipients and the data subject?
- b) What harm will come to the individuals because of the breach? Harm may include:
 - (i) *security risk (e.g. physical safety)*
 - (ii) *identity theft or fraud*
 - (iii) *loss of business or employment opportunities*
 - (iv) *hurt, humiliation, damage to reputation or relationships*
- c) What harm could result to the public body or organization because of the breach?
 - (i) *loss of trust in the public body or organization*
 - (ii) *loss of assets*
 - (iii) *financial exposure*
- d) What harm could result to the public because of the breach? For example:
 - (i) *risk to public health*
 - (ii) *risk to public safety*

5.12.4.3 Step 3: Notification

The key consideration overall in deciding whether to notify should be if notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately collected, used or disclosed.

Review your risk assessment to determine whether notification is appropriate. The ATIPP Office has created a *Privacy Breach Notification Assessment Tool* to assist public bodies in determining when and how to notify individuals.

1) Notifying Affected Individuals

As noted above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm. Some considerations in determining whether to notify individuals affected by the breach include:

- *Contractual obligations require notification*
- *There is a risk of identity theft or fraud (usually because of the type of information lost, such as SIN, banking information, identification numbers)*
- *There is a risk of physical harm (if the loss puts an individual at risk of stalking or harassment)*
- *There is a risk of hurt, humiliation or damage to reputation (for example when the information lost includes medical or disciplinary records)*

2) When and How to Notify

When: Notification of individuals affected by the breach should occur as soon as possible following the breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether to delay notification so as not to impede a criminal investigation.

How: The preferred method is direct notification is direct (by phone, letter or in person) to affected individuals. Indirect notification (website information, posted notices, media) should generally only occur where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking. In certain cases, using multiple methods of notification may be the most effective approach.

3) What should be included in the notification?

Notifications should include the following pieces of information:

- *Date of the breach*
- *Description of the breach*
- *Description of the information inappropriately accessed, collected, used or disclosed*
- *Steps taken so far to mitigate the harm*
- *Next steps planned and any long term plans to prevent future breaches*
- *Steps the individual can take to further mitigate the risk of harm*
- *Contact information of an individual within the public body or organization who can answer questions or provide further information*
- *Contact information for the Office of the Information and Privacy Commissioner, to whom individuals have the right to issue a complaint regarding a breach of privacy.*

4) Others to Contact

Regardless of the approach taken to notifying individuals, public bodies should consider whether the following authorities or organizations should be informed of the breach:

- **Police:** *if theft or other crime is suspected*
- **Insurers or others:** *if required by contractual obligations*
- **Professional or other regulatory bodies:** *if professional or regulatory standards require notification of these bodies*
- **ATIPP Office:** *to provide advice or guidance in regard to the privacy breach*

5.12.4.4 Step 4: Prevention

Once immediate steps are taken to mitigate the risks associated with the breach, you need to take the time to investigate the cause of the breach. This could require:

- *A security audit of both physical and technical security; because of this evaluation, you should develop or improve, as necessary, adequate long-term safeguards against further breaches*
- *Policies should be reviewed and updated to reflect the lessons learned from the investigation and regular review of policies should be implemented*
- *An audit at the end of the investigation process to ensure that the prevention plan has been fully implemented*
- *Training of public body staff to ensure organizational understanding of a public body's privacy obligations under the ATIPP Act*

Appendices

| | |
|--------------------------------------------------------------|------------|
| Appendix A: Information Sharing Agreement (ISA) | 41 |
| Appendix B: Generic Privacy Notice | 45 |
| Appendix C: Annual Privacy Checklist | 46 |
| Appendix D: PIA Policy | 56 |
| Appendix E: PIA Protocol | 67 |
| Appendix F: Preliminary PIA | 69 |
| Appendix G: PIA Template (Annotated) | 81 |
| Appendix H: Privacy Breach Protocol | 123 |
| Privacy Breach Handout | |
| Privacy Breach Reporting Form | |
| Key Steps When Responding to a Privacy Breach | |
| Privacy Breach Notification Assessment Tool | |

Please note that documents contained in the Appendices may have been updated since publication of this Privacy Manual. For updated versions, contact your Senior Privacy Analyst in the ATIPP Office.

Appendix A: Information Sharing Agreement (ISA)

INFORMATION SHARING AGREEMENT (ISA) TEMPLATE

1.0 Purpose

The Information Sharing Agreement (ISA) will provide for the exchange of personal information between [Party X] and <Public Body> for the purpose of: <List ALL purposes below>

1.1 <Party X> needs information from <Public body> for the purpose of establishing <Detailed information about program/service/project>

2.0 Authority to Disclose Information

2.1 The information needed by <Party X> from <Public Body> for the purpose of <program/service/project> is authorized under <section(s) of an Act(s)>

2.2 Similarly, <Public Body> is authorized to disclose the information outlined in this ISA to <Party X> under section(s) <insert disclosure section(s)> of the Access to Information and Protection of Privacy (ATIPP) Act

3.0 Information to be Exchanged

3.1 <Public Body> will provide <Party X> with the following information from <insert where information will be retrieved from (i.e. a system or file)> for the purpose of <program/service/project>.

- <List information>:
- SAMPLE:
- name
- social insurance number
- address
- date of birth
- Etc...

4.0 Mechanism for Exchange of Information

4.1 Information covered by this ISA will be provided by <Public Body> in a mutually agreed format and manner. In this regard, <Public Body> agrees to disclose information by way of <format and manner>

4.2 The parties agree that whatever option is chosen, access to information covered by this ISA will be:

(a) Limited to only those employees, agents or contractors who require access for the purposes listed in clauses <List> and will only be used for the purposes listed in clauses <list>. In addition, <Party X> agrees that they will limit access to this information to the minimum amount of personal information required to achieve the intended purpose.

5.0 Confidentiality and Use

5.1 <Party X> will maintain, respect and protect the confidentiality of the information received under this ISA, and will not use or disclose it to anyone for any purpose without the written consent of the <Public Body> providing the information, other than:

- (a) for those purposes specifically mentioned in <insert>
- (b) for a consistent purpose, as defined in section <insert> of the ATIPP Act and in accordance with the Government of Newfoundland and Labrador guidelines and policies;
- (c) for a purpose authorized or required by law, including those disclosures authorized under section <insert> of the ATIPP Act.

5.2 The parties acknowledge that, where consent to use or disclose personal information is a requirement for program/service/project, written authorization will be obtained and individuals will be notified of the purpose for the use or disclosure.

6.0 Information Management

6.1 The information exchanged under this ISA shall be collected, administered, maintained, destroyed or disposed of in accordance with:

(a) The ATIPP Act and Regulations; the Records Management Regulation from the Office of the Chief Information Officer (OCIO) and any related data security and retention of records directives, policies and guidelines covering the administrative, technical and physical safeguarding of the personal information.

6.2 The Information Management (IM) arrangements above will ensure the confidentiality and , integrity of personal information covered under this ISA and will safeguard the personal information against accidental or unauthorized access, disclosure, use, modification and deletion.

6.3 <Party X> will promptly notify the <Public Body> of any unauthorized access, use or disclosure and will furnish the <Public Body> with full details of the incident.

6.4 In the event of an occurrence described in clause 6.3 above, <Party X> will promptly take all reasonable steps to prevent a recurrence of the unauthorized event. Additionally, <Public Body> reserves the right to cease sharing information if it is determined appropriate to do so.

7.0 Accuracy

7.1 <Public Body> will, to the best of its ability, ensure the completeness and accuracy of the information provided to <Party X> under this ISA. However, it is understood and agreed that they cannot guarantee its accuracy and will, therefore, not be held responsible for any damage resulting from the transmission or use of any information that is inaccurate or incomplete.

7.2 <Public Body> and <Party X> agrees to review any requests from individuals for correction of their personal information that may be in the custody or under the control of that party, in accordance with the ATIPP Act.

8.0 Office of the ATIPP Coordinator

8.1 If an issue arises as to whether the provisions of the ATIPP Act apply to certain personal information covered in this ISA, the parties may consult with the Office of the ATIPP Coordinator.

Contact:

Access to Information and Protection of Privacy Office
Department of Justice
4th Floor, East Block
Confederation Building
P.O. Box 8700
St. John's, NL
A1B 4J6

Fax: (709) 729 -5466
Phone: (709) 729-7072

9.0 Ensuring Data Protection

9.1 The parties agree that they are responsible for the actions of their own employees, agents and contractors with respect to the collection, use, disclosure, retention, and disposal of personal information in their custody or under their control, regardless if the person is or was acting within the scope of his or her employment, agency or contract.

9.2 The parties will, separately or jointly, conduct a periodic review of Information Management practices and procedures outlined under this ISA to ensure compliance with the provisions of the ATIPP Act.

10.0 General

10.1 This ISA can be modified with the written consent of designated officials of <Public Body> and <Party X>.

11.0 Expiry

11.1 This ISA will expire on <date>.

12.0 Sign-Off

12.1 Agreed to on behalf of *<Public Body>*:

<Name of Authorized Individual>

<Title of Authorized Individual>

<Address>

<Telephone Number>

<Fax Number>

<Email>

12.2 Agreed to on behalf of *<Party X>*:

<Name of Authorized Individual>

<Title of Authorized Individual>

<Address>

<Telephone Number>

<Fax Number>

<Email>

12.3 Date

<Insert date>

Appendix B: Generic Privacy Notice

Privacy Notice

Under the authority of the **<insert name of your Act or program>**, personal information will be collected for the purpose of **<insert>**. Section **<insert section #>** of the **<insert name of Act>** allows **<insert public body>** to disclose personal information to **<insert>** for the purpose of **<insert purpose>**.

Any questions or comments can be directed to **<insert contact title/contact information>** or **<web address>**.

In accordance with the *ATIPP Act*, privacy notices should state 3 things:

1. The purpose of the collection
2. The authority* for the collection (the Act or Program)
3. The contact information** of someone who can answer questions about the collection

**ATIPPA allows personal information to be collected if it is 'necessary for an operating program or activity', so you can name the associated program as your authority.*

***Contact information does not need to include an individual's name, but it should list a title and a contact number*

Appendix C: Annual Privacy Checklist

Division / Department / Agency / Program

Contact Name

Contact Title

Contact Email

Contact Telephone Number

Does your department / division / program exchange personal information with other departments or agencies of the Government of Newfoundland and Labrador? If so, please indicate which departments or agencies are involved. Please check all that apply.

| | |
|--|------------------------------------------------|
| | Business |
| | Education |
| | Environment and Conservation |
| | Executive Council |
| | <i>Cabinet Secretariat</i> |
| | <i>Intergovernmental Affairs Secretariat</i> |
| | <i>Public Service Secretariat</i> |
| | <i>Office of the Chief Information Officer</i> |
| | <i>Women's Policy Office</i> |
| | <i>Rural Secretariat</i> |
| | Finance |
| | Fisheries and Aquaculture |
| | Government Services |
| | Health and Community Services |
| | Human Resources, Labour and Employment |
| | Innovation, Trade and Rural Development |
| | Justice |
| | Labrador and Aboriginal Affairs |
| | Municipal Affairs |
| | Natural Resources |

- Tourism, Culture and Recreation
- Transportation and Works
- Other agency (please specify below)

Does your department / division / program exchange personal information with any persons or organizations outside the Government of Newfoundland and Labrador? If so, please indicate which types of persons or organizations are involved. Please check all that apply.

Not Applicable: No exchange of personal information outside the GNL.

- Private individuals
- Contracted service providers or vendors
- Other levels of government within Newfoundland and Labrador
- Other provincial governments
- Law enforcement agencies
- Government of Canada
- Other (please specify)

Please list information exchanged and relationships.

Does your division / program outsource any functions related to the collection, storage, or management of personal information?

- Yes
- No
- Unknown / Other (please elaborate)

Are there information security measures implemented around your collections of personal information?

- Security assessments for new projects and systems
- Security audits for existing projects and systems
- Physical access controls, such as locked file cabinets and storage rooms
- Electronic access controls, such as user authentication and authorization, intrusion protection measures, and access logs.
- Information integrity measures, such as accuracy reviews, logical edits for data entry systems, and other measures to ensure that personal information is accurate and up-to-date.
- Measures to ensure the availability of personal information, such as backup procedures (on-site and off-site), disaster recovery plans, etc.
- No
- Not Applicable

| | |
|--|-----------------|
| | Unknown / Other |
| | |

What kinds of personal information does your department/division/program COLLECT?
(ATIPPA S.33)

| | |
|--|-------------------------------|
| | name |
| | home address |
| | home telephone |
| | race |
| | national origin |
| | ethnic origin |
| | skin colour |
| | religious beliefs |
| | religious associations |
| | political beliefs |
| | political associations |
| | Date of Birth |
| | age |
| | sex |
| | sexual orientation |
| | marital status |
| | family status |
| | identifying number |
| | identifying symbol |
| | other identifying particular |
| | fingerprints |
| | blood type |
| | inheritable characteristics |
| | health care status or history |
| | physical disabilities |
| | mental disabilities |
| | educational status or history |
| | financial status or history |
| | employment status or history |
| | criminal status or history |

| | |
|--------------------------|---------------------------------------------|
| <input type="checkbox"/> | family status |
| <input type="checkbox"/> | identifying number |
| <input type="checkbox"/> | identifying symbol |
| <input type="checkbox"/> | other identifying particular |
| <input type="checkbox"/> | fingerprints |
| <input type="checkbox"/> | blood type |
| <input type="checkbox"/> | inheritable characteristics |
| <input type="checkbox"/> | health care status or history |
| <input type="checkbox"/> | physical disabilities |
| <input type="checkbox"/> | mental disabilities |
| <input type="checkbox"/> | educational status or history |
| <input type="checkbox"/> | financial status or history |
| <input type="checkbox"/> | employment status or history |
| <input type="checkbox"/> | criminal status or history |
| <input type="checkbox"/> | anyone else's opinions about the individual |
| <input type="checkbox"/> | the individual's views or opinions |
| <input type="checkbox"/> | Not Applicable / None |
| <input type="checkbox"/> | Unknown / Other (please elaborate below) |
| | |

What kinds of personal information does your division / program DISCLOSE ? Check all that apply. (ATIPPA S.39)

| | |
|--------------------------|------------------------|
| <input type="checkbox"/> | name |
| <input type="checkbox"/> | home address |
| <input type="checkbox"/> | home telephone |
| <input type="checkbox"/> | race |
| <input type="checkbox"/> | national origin |
| <input type="checkbox"/> | ethnic origin |
| <input type="checkbox"/> | skin colour |
| <input type="checkbox"/> | religious beliefs |
| <input type="checkbox"/> | religious associations |
| <input type="checkbox"/> | political beliefs |
| <input type="checkbox"/> | political associations |
| <input type="checkbox"/> | Date of Birth |
| <input type="checkbox"/> | age |

| | |
|--------------------------|---------------------------------------------|
| <input type="checkbox"/> | sex |
| <input type="checkbox"/> | sexual orientation |
| <input type="checkbox"/> | marital status |
| <input type="checkbox"/> | family status |
| <input type="checkbox"/> | identifying number |
| <input type="checkbox"/> | identifying symbol |
| <input type="checkbox"/> | other identifying particular |
| <input type="checkbox"/> | fingerprints |
| <input type="checkbox"/> | blood type |
| <input type="checkbox"/> | inheritable characteristics |
| <input type="checkbox"/> | health care status or history |
| <input type="checkbox"/> | physical disabilities |
| <input type="checkbox"/> | mental disabilities |
| <input type="checkbox"/> | educational status or history |
| <input type="checkbox"/> | financial status or history |
| <input type="checkbox"/> | employment status or history |
| <input type="checkbox"/> | criminal status or history |
| <input type="checkbox"/> | anyone else's opinions about the individual |
| <input type="checkbox"/> | the individual's views or opinions |
| <input type="checkbox"/> | Not Applicable / None |
| <input type="checkbox"/> | Unknown / Other (please elaborate below) |

Does your division / program DISCLOSE personal information not included in the list above?

| | |
|--------------------------|----------------------------------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Unknown/Other (please elaborate below) |

How is the collection of personal information authorized? (ATIPPA S.32) Check all that apply.

| | |
|--------------------------|---------------------------------------------------------------------------------|
| <input type="checkbox"/> | Authorized by an Act of Newfoundland and Labrador or of Canada |
| <input type="checkbox"/> | Collected for the purposes of law enforcement |
| <input type="checkbox"/> | Information relates directly to general enabling legislation of the public body |
| <input type="checkbox"/> | Not Applicable |

| | |
|--------------------------|------------------------------------------|
| <input type="checkbox"/> | Unknown / Other (please elaborate below) |
| <input type="text"/> | |

Is any personal information collected for which explicit authorization is unclear or does not exist?

| | |
|--------------------------|------------------------------------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate below) |
| <input type="text"/> | |

How does your department/divisions/program collect personal information? Check all that apply.

| | |
|--------------------------|----------------------------------------------------------------|
| <input type="checkbox"/> | Directly from the person who is the subject of the information |
| <input type="checkbox"/> | Directly from a third party |
| <input type="checkbox"/> | Via secondary sources |
| <input type="checkbox"/> | Via data matching |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate below) |
| <input type="text"/> | |

When collecting personal information directly from the individual, is he or she: (ATIPPA S.33)

| | |
|--------------------------|----------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Informed of the purpose of collection and the legal authority for it |
| <input type="checkbox"/> | Provided with contact information for a person to whom he or she may address questions |
| <input type="checkbox"/> | Asked to consent to the collection |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate below) |
| <input type="text"/> | |

When collection is NOT to be directly from the individual, will collection be authorized by any or all of the following: (ATIPPA S.33)

| | |
|--------------------------|------------------------------------------|
| <input type="checkbox"/> | The ATIPP Act |
| <input type="checkbox"/> | The individual |
| <input type="checkbox"/> | Another Act or regulation |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate below) |
| <input type="text"/> | |

Are means provided to keep personal information accurate, complete and up-to-date as needed for its intended purposes? (ATIPPA S.34)

| | |
|--------------------------|------------------------------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate) |

Is personal information retained for at least one year? (ATIPPA S.37)

| | |
|--------------------------|------------------------------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate) |

Are subjects able to request correction of their personal information? (ATIPPA S.35)

| | |
|--------------------------|------------------------------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate) |

Is personal information protected against such risks as loss or unauthorized access, collection, use, disclosure, destruction, or modification? (ATIPPA S.36)

| | |
|--------------------------|------------------------------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate) |

If so, please summarize the security measures that are applied.

Is personal information disclosed only for purposes consistent with the original purpose of collection? (ATIPPA S.39)

| | |
|--------------------------|------------------------------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate) |

If there is to be disclosure for any other purposes, please list those purposes, one per line.

[Redacted]

Has your area identified and documented which paper-based and electronic systems contain personal information or personal health information?

- Yes
- No
- Not Applicable - Do not collect personal or personal health information

Do you provide staff with training about privacy?

- Yes
- No

How quickly can records containing personal information be identified and retrieved when required? Check the closest response.

- Usually within one day
- Usually within one week
- Usually within one month
- It could often take more than a month
- Unknown/Other (please elaborate below)

[Redacted]

Have any persons outside the Department ever expressed concern about the loss or absence of records, poor response to requests for information, or unauthorized access or release? If yes, please give examples.

- Yes
- No
- Unknown/Other

Please elaborate below:

[Redacted]

Have formal instructions been issued to staff and contractors about access to records?

- Yes
- No
- Unknown/Other

Please elaborate below:

[Redacted]

If yes, do the instructions cover both paper and electronic records? Please attach the instructions.

- Yes
- No
- Not applicable
- Unknown/Other

Please elaborate below:

Are any records (paper and/or electronic) maintained by individual staff and accessible only to them (as opposed to a shared location, such as a registry or network)?

| |
|--|
| |
| |
| |

Yes

No

Unknown/Other

Please elaborate below:

Please add any additional comments you would like to provide here.

DECLARATION OF NO PERSONAL INFORMATION

IMPORTANT: In completing this section, you acknowledge that after a complete review and analysis of the Annual Privacy Checklist, this Department/Division/Program DOES NOT COLLECT, USE, DISCLOSE, STORE or MANAGE personal information.

The Senior Privacy Analyst assigned to your Department will follow up to confirm that no personal information is collected, used, disclosed, stored or managed, as stated in this Declaration. Please provide the following contact information - all fields are MANDATORY:

Division / Department / Agency / Program

Contact Name

Contact Title

Contact Email

Contact Telephone Number

Appendix D: PIA Policy

Government of Newfoundland and Labrador
Privacy Impact Assessment Policy

Preamble

A privacy impact assessment (PIA) is an evaluation process which allows those involved in the collection, use or disclosure of Personal Information to assess and evaluate privacy, confidentiality or security risks associated with these activities, and to develop measures intended to mitigate the identified risks.

Definitions

- **ATIPP Act** means the *Access to Information and Protection of Privacy Act* of Newfoundland and Labrador.
- **Department** means a Department of the Government of Newfoundland and Labrador, or any other Public Body under the province's *Access to Information and Protection of Privacy Act* that reports to a minister of the provincial government.
- **Office of the ATIPP Coordinator** means the Government of Newfoundland and Labrador office responsible for the administration of the ATIPP Act. It is to be distinguished from Departmental ATIPP coordinators, who are responsible for managing the access provisions of the ATIPP Act for individual Departments.
- **Personal Information** has the same meaning as in the *Access to Information and Protection of Privacy Act*.
- **PIA** means "privacy impact assessment".
- **PIA Template** means the questionnaire and any related automated tools provided by the Office of the ATIPP Coordinator to support the completion of a privacy impact assessment for a Project.
- **Privacy Lead** means a person in a Department who has been designated the role of coordinating privacy compliance activities and privacy impact assessment within that Department.
- **Privacy Checklist** means the checklist and any future related automated tools provided by the Office of the ATIPP Coordinator and/or the Office of the Chief Information Officer for the preliminary assessment of ATIPP Act compliance associated with a Project and to determine the need for a PIA.
- **Privacy Impact Assessment (PIA)** is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use or disclosure of Personal Information. It may also define the measures used to mitigate and, wherever possible, eliminate the identified risks.
- **Project Manager** means the person with primary operational responsibility for ensuring that the Project is brought to a successful conclusion.
- **Project** means 'scheme', 'program', 'initiative', 'application', 'system', or any other formally defined course of endeavour.
- **Public Body** has the same meaning as in the *Access to Information and Protection of Privacy Act*.

Policy Statement

Public Bodies within the Government of Newfoundland and Labrador will conduct PIAs for all new and significantly redesigned collections, uses or disclosures of Personal Information that may raise potential privacy risks.

PIA Process

The PIA process ensures that measures intended to protect privacy and ensure the confidentiality and security of Personal Information are considered at the outset of any new program or service delivery initiative.

A privacy impact assessment shall consist of:

- A specific assessment against the privacy provisions of the *Access to Information and Protection of Privacy Act*;
- A data flow description for the collection, use or disclosure of Personal Information; and
- A threat and risk assessment of the collection, use or disclosure of Personal Information.

Privacy impact assessments shall be conducted using the procedures, checklists, tools and templates developed by the Office of the ATIPP Coordinator and, insofar as information technology assessments or features may be required, by the Office of the Chief Information Officer.

In some cases, such as those involving legacy information systems, it is possible that full compliance with ATIPP privacy provisions may not be immediately achievable. As part of the PIA report, Public Bodies should specify the time frame within which they expect to achieve full privacy compliance for the Project that is the subject of the PIA.

Roles and Responsibilities

Public Body

The Head of the Public Body is responsible for compliance with the privacy provisions of the *Access to Information and Protection of Privacy Act*.

Public Bodies within the Government of Newfoundland and Labrador shall be responsible for the review of all new and significantly redesigned collections, uses and disclosures of Personal Information to determine whether proposed programs or systems conform to the privacy provisions of the *Access to Information and Protection of Privacy Act*.

The Department Head or delegate responsible for the program or system under consideration shall ensure that a privacy impact assessment is completed in accordance with this policy. When completed, the PIA shall be reviewed and approved by the Department Head, or by a person designated in writing by him or her to review and approve PIAs.

PIAs involving information technology Projects or initiatives under the responsibility of the OCIO shall also be approved by the Chief Information Officer, or by a person designated in writing by him or her to review and approve PIAs.

Office of the ATIPP Coordinator

The Office of the ATIPP Coordinator shall be responsible for:

- Developing and maintaining the privacy impact assessment process and procedures;
- Ensuring that the process and procedures are understood throughout the Government of Newfoundland and Labrador; and
- Assisting departments in completing privacy checklists and PIAs.

Changes to this policy and related processes and procedures shall be subject to the approval process instituted by the minister responsible for the Office of the ATIPP Coordinator.

Chief Information Officer (CIO)

The CIO shall be responsible, in cooperation with the responsible Public Body or bodies, for the review and approval of privacy impact assessments involving the use of information technology where the Office of the CIO has jurisdiction. The Office of the CIO does not have responsibility of all IT systems and operations in the public sector. The CIO shall also be responsible for ensuring that security threat and risk assessments are undertaken as necessary to comply with Section 36 of the *Access to Information and Protection of Privacy Act*, and that appropriate measures are taken to secure Personal Information.

The Office of the CIO shall incorporate privacy impact assessments into its project management standards, in cooperation with the Office of the ATIPP Coordinator.

The Office of the CIO shall be the lead agency in addressing technical components of privacy issues.

Project Manager

Project Managers, designated by either the public body or the OCIO, shall be responsible for ensuring the privacy impact assessment is completed and may be involved in conducting the privacy impact assessment and overseeing the process. If the Project does not have a Project Manager assigned, the manager who otherwise carries day-to-day responsibility for the Project is responsible for conducting the privacy impact assessment.

The Project Manager shall undertake privacy impact assessments in accordance with the relevant PIA procedures and best practices.

PIA Procedures and Best Practices

Circumstances Requiring a PIA

The project-based Privacy Checklist, which is discussed later, provides guidance concerning the necessity of a PIA for a specific Project. In general, though, a privacy impact assessment may be indicated when one or more of the following conditions apply:

- Personal information will be collected that has not previously been collected, or previously collected Personal Information will be collected for a new or different purpose;
- Previously collected Personal Information will be used for a purpose that is not directly related to the purpose of the original collection;
- Personal information will be disclosed to a recipient and/or for a purpose that is not explicitly authorized in legislation;
- The retention, disposition, storage or management of Personal Information will change substantially, or will be performed by a new organization or application; or
- The collection, storage, use or disclosure of Personal Information will be performed by a third party under contract.

Exceptions to the above conditions require the approval of the Office of the ATIPP Coordinator. The Privacy Checklist will address these issues and others related to compliance requirements arising from the *Access to Information and Protection of Privacy Act*.

*The Privacy Checklist must be completed for any new Project or initiative undertaken by a Department or agency of the Government of Newfoundland and Labrador. The results of the Privacy Checklist must be considered in deciding whether a full privacy impact assessment is required. If recommendations arising from the Privacy Checklist include a recommendation to undertake a full privacy impact assessment, any decision **not** to do so must be stated in writing over the signature of the responsible deputy minister and filed with Project documentation.*

The Privacy Checklist assesses factors related to compliance requirements in the ATIPP Act. In addition, however, other privacy risks may arise in areas that may not be explicitly addressed in the ATIPP Act. Although they are not necessarily explicit, if they are not recognized they can nevertheless lead to compliance problems, or to perceived deficiencies in privacy protection on the part of affected individuals, decision-makers, or the public at large. The latter can sometimes be as problematic as the former.

Some common privacy risks include the following:

- *Data profiling/data matching*: combining unrelated Personal Information obtained from a variety of sources to create new information about an individual or using information about an individual's preferences and habits to build a profile on the individual;
- *Transaction Monitoring*: observing or tracking the history of an individual's interaction with one or more programs or services. This usually results in creation of new Personal Information describing an individual's overall experience with one or more programs;
- *Identification of Individuals*: electronic service delivery generally requires identification of an individual and authentication of their identity as way of managing security risks. Surveillance risks exist where the use of common identifiers or identification systems facilitate data sharing, profiling or transaction monitoring;

- *Physical observation of individuals:* tracking the movement or location of an individual through the use of vehicle transponders, satellite locators, cameras or mechanisms for recording an individual's use of kiosks;
- *Publishing or re-distribution of public databases containing Personal Information:* electronic publishing frequently eliminates practical limits on the misuse of information, as it can be easily manipulated and used for purposes entirely unrelated or is intended use in manual form; and
- *Lack or Doubtful Legal Authority:* failure to identify clear program authority to collect, use or disclose Personal Information raises concerns about whether an initiative should be undertaken on both the privacy front and, sometimes, with respect to the *Charter of Rights and Freedoms Act*.

These and any other relevant factors should be considered in combination with the results from the Privacy Checklist, to determine whether a full privacy impact assessment is indicated for the Project under consideration.

PIA Roles and Responsibilities in Detail

Office of the Information and Privacy Commissioner

The Office of the Information and Privacy Commissioner is not normally involved in the PIA process. The involvement of the commissioner's office in a PIA review can compromise the commissioner's objectivity in the event of a subsequent complaint.

The commissioner should be consulted whenever there are privacy issues for which such consultation could be helpful, but should not be asked to review PIAs.

Office of the ATIPP Coordinator

The government's central access to information and privacy (ATIPP) office is responsible for the PIA policy, any related guidelines, a standardized format for the PIA document and any related tools or checklists.

This does not preclude the ability of individual Departments³ to implement additional, optional privacy assessment procedures that are specific to their needs, but any such procedures must be consistent with government-wide policy and procedures. Consistency in the PIA process is critical for its continued effectiveness over the long term.

The Office of the ATIPP Coordinator is responsible for privacy training and awareness materials and related activities for the Government of Newfoundland and Labrador. The Office of the ATIPP Coordinator will consult with the office of the CIO related to technical areas or issues as necessary.

In general, the Office of the ATIPP Coordinator has the following responsibilities related to privacy administration and privacy impact assessment:

- Corporate training regarding privacy legislation impact on Departments;
- Policy development and review, including PIA standards;
- Trouble shooting and expertise in the area of corporate compliance with privacy legislation;
- Support to Departments;
- Annual reporting to the Legislature of government-wide compliance activities and status;
- Developing high level reporting formats (i.e. number of PIAs done, summary of issues and corrective action) for Departments to use in support of reporting to the Legislature;
- Liaising with the Privacy Commission when complaints have been received through the Commissioner's Office; and
- Maintaining a repository of completed PIAs.

Office of the Chief Information Officer

³ We use the term "Department" to mean a Department of the provincial government or any other Public Body under the ATIPP Act whose chief executive officer reports to a minister of the provincial government.

The Office of the Chief Information Officer has a critical role to play in the privacy impact assessment process as it relates to information technology Projects and initiatives. It must ensure that IT Projects are undertaken in full consideration of the privacy requirements facing information technology applications. As specified in the *Privacy Impact Assessment Policy*, the office of the CIO will incorporate privacy impact assessment into its project management standards, in cooperation with the Office of the ATIPP Coordinator.

Project management standards should specify the stage of the Project at which a privacy impact assessment is conducted, as well as any IT specific requirements associated with the PIA process. It is a best practice to undertake PIA works as early as possible in a project.

In the information technology realm, privacy and security are inextricably intertwined. However, that does not mean that they cannot operate at cross purposes. It is therefore critical that the privacy impact assessment process be coordinated with the security threat and risk assessment process. One implication of the need for such coordination is that the security threat and risk assessment process also needs to be incorporated into project management standards.

The office of the CIO is the lead agency in addressing privacy issues from a technical perspective. This may involve actively soliciting ideas or solutions for the protection of Personal Information, such as improved security measures, anonymization techniques, access control improvements, and privacy enhancing technologies.

The development of privacy standards for information technology applications will make the process of privacy impact assessment for such applications much easier. With IT privacy standards in place, the privacy impact assessment has a clear reference point from which to evaluate the more technical aspects of privacy protection.

Like security standards, privacy standards can offer a way to agree on the measures to be taken to minimize privacy risks associated with IT applications. Unlike security standards, IT privacy standards are not currently available from international standards organizations, although efforts are underway to develop them. In the meantime, the Government of Newfoundland and Labrador would benefit from working towards developing privacy standards for incorporation into overall IT design requirements.

In general, the office of the CIO is responsible for:

- Developing IM, and infrastructure strategies to incorporate corporate information compliance with privacy legislation;
- Identifying existing, systems which require PIAs, such as important legacy systems and those scheduled for update or replacement;
- Participating in PIAs in conjunction with Departments and approving PIA results when they involve information technology for which the CIO is responsible;
- Developing solutions to fix privacy vulnerabilities and risks in so far as they are related to current applications of information technology, information management and infrastructure;
- Integrating privacy impact assessment into new systems development via the project management framework; and
- Consulting to client Departments on technical aspects of privacy in terms of IM and Infrastructure, including the application of privacy enhancing technologies.

Departments

The responsibility for privacy compliance ultimately rests on the shoulders of ministers of the Crown. Therefore, individual Departments must take responsibility for ensuring that their services, projects and initiatives meet the requirements of privacy legislation and the fair information practices upon which that legislation is based.

Department Heads carry all ATIPP responsibilities on behalf of their Departments. Department Heads may delegate responsibilities under the ATIPP Act, but the Head's delegates may not further delegate those responsibilities unless the Act specifically states that they may. Although delegates may assign duties related to ATIPP responsibilities to others, they cannot delegate the responsibility for completing those duties. This means that Department Heads must carefully delegate ATIPP responsibilities to be sure that delegated persons or positions are the appropriate ones to carry the related responsibilities.

Since departments are ultimately responsible for privacy compliance, final approval of privacy impact assessment results and any actions resulting from those results must lie with the responsible Department or Departments, including the Department responsible for the Office of the CIO in cases of joint information technology projects.

The PIA process for information technology projects takes into account the role of individual Departments in projects involving multiple Departments. It does so in a way that meets Departmental requirements for privacy due diligence, but coordinates PIA efforts to minimize duplication of effort in the conducting of the PIA and the review of its results. A similar process can be used for non-IT projects involving multiple Departments.

Departmental responsibilities for the PIA process are vested in the responsible Department Head or designated delegate

Projects involving multiple Departments may involve some uncertainty regarding which Department should have overall responsibility for ensuring that PIA requirements are met. Most such Projects will have a steering committee or some other interdepartmental structure to provide direction to the Project.

For interdepartmental Projects, the Department that provides the chairperson for the steering committee or other interdepartmental structure governing the Project should be accountable for ensuring that all necessary privacy processes take place. Note that this does not in any way change or diminish the accountability of individual Departments for ATIPP compliance.

In general, Departments are responsible for the following PIA-related functions:

- Identifying privacy vulnerabilities and privacy related issues related to specific areas of Departmental responsibility;
- Conducting the Privacy Checklist for projects managed by the Department (see Project Manager responsibilities below);
- Assigning business priorities for existing systems and processes that may require privacy impact assessments, in consultation with the OCIO where information technology systems are involved;
- Initiating a PIA whenever the Department has privacy concerns about a Project in which it is participating. (In Projects involving multiple Departments, it is recommended that any participating Department have the authority to initiate a PIA if it believes one to be necessary);

- In conjunction with the ATTIP Office, ensuring the delivery of privacy training and information to Department staff and the participation of staff in that training;
- Approving PIA results and recommendations; approvals should be rendered by the deputy minister or someone the deputy minister has delegated in writing to approve PIAs; and
- Collaborating with the Office of the CIO to complete PIAs on information technology projects.

Project Managers

Many PIAs will be conducted as part of project management and many of these projects will be technology projects that involve the OCIO. The project manager can be either from a public body, or the OCIO. Project managers are essential in the successful completion of any privacy impact assessment. In cases where the project manager is provided from the OCIO, he or she will most likely have the necessary knowledge and experience to know where potential privacy risks and issues may lie. In cases where the project manager is from the client department, he or she may not have sufficient privacy expertise to identify privacy issues and may have to rely on the knowledge and experience of an OCIO representative (in the case of a technology project), or the business owner.

If privacy is to be properly incorporated into the Project and its management, the Project Manager must take the lead role in performing the privacy impact assessment. The greatest value of a PIA is in the process of conducting it and the things learned during that process, not in the report produced.

The Project Manager should be the lead agent in conducting the privacy impact assessment, with the guidance of the privacy analyst from the ATTIP Office and/or outside agencies, as appropriate, and reporting via the project management structure to the responsible Department Head or delegate(s).

In those cases in which the Project Manager is a contracted resource, the departmental manager for that contract should be the lead agent for the PIA.

The Project Manager has the following responsibilities related to the Privacy Checklist and PIA:

- Completing the Privacy Checklist, or ensuring that it is completed;
- Assessing recommendations and findings arising from the Privacy Checklist and making recommendations regarding the need for a full privacy impact assessment to senior management responsible for the Project;
- If a full PIA is to be undertaken, assembling and leading a PIA team in accordance with the procedures and best practices elsewhere in this document and ensuring that the team includes all necessary representation and expertise;
- Determining the need for outside expert assistance, if any, and coordinating activities to obtain such assistance if necessary;
- Leading the development of a PIA work plan by the PIA team with advice from the privacy analyst of the ATTIP Office;
- Managing the implementation of the PIA work plan, including the necessary approvals;

-
- Managing the PIA process as it unfolds;
 - Liaising with external stakeholders and interested parties as necessary throughout the PIA process;
 - Supervising the preparation of draft and final PIA reports;
 - Supervising the preparation of the PIA implementation plan by the PIA team; and
 - Reporting to participating Departments and the Office of the CIO as necessary.

Project Staff

Project staff (from both a public body and, as appropriate, the OICO) will ultimately be responsible for implementing the recommendations arising from the privacy impact assessment. Therefore, they should be involved in the PIA process to the extent necessary to understand the genesis of the resulting recommendations and their impact on the Project. Project staff will often be called upon to participate in the PIA team.

Much of the information required for the PIA will have to be provided by Project staff. It is therefore important that sufficient staff time be allocated to the privacy impact assessment to ensure its successful completion.

Project staff has three important roles in privacy impact assessment. The first is to provide information and documentation to support the PIA. The second is to participate in the PIA team as necessary. The third role comes after the completion of the PIA. Project staff will be responsible for implementing most, if not all, of the recommendations arising from the PIA report. It is therefore important that the reason for these recommendations and the decision process behind them be well understood by Project staff. Without such understanding, recommendations may be implemented improperly, incompletely, or inappropriately.

For example, security personnel who are unfamiliar with privacy requirements may mistakenly conclude that security measures recommended in a PIA report can be replaced by other security measures that they consider to be functionally equivalent but easier to implement. Such conclusions are rarely valid, but security personnel have no way of knowing that unless they are cognizant of the privacy issues that the proposed measures are intended to address. Project staff has the following responsibilities related to the PIA process:

- Actively supporting or participating in the PIA team as necessary;
- Providing information and documentation as necessary to support the PIA process from their respective areas of expertise and organizational roles;
- Exercising considered, professional judgment in the conduct of the PIA and the preparation of related findings;
- Providing support to external experts as necessary, if such experts are engaged in the PIA;
- Notifying the Project Manager of any problems or issues related to the PIA as soon as they are known;
- Ensuring that the views of their respective business areas, Departments or agencies are fully represented on the PIA team and in its deliberations;

- Liaising with others in their respective business areas, Departments or agencies as necessary to support the successful completion of the PIA;
- Actively participating in the preparation and implementation of the PIA implementation plan;
- Providing post-PIA follow-up and monitoring as necessary and appropriate.

The complete **PIA Policy and Procedure Manual** is available from the ATIPP Office.

Appendix E: PIA Protocol

PIA Protocol for IT Projects

| PIA & PPIA Protocol | Who? | What? | When? | Department | ATIPP Office | Information Protection (IP) Analyst, OCIO |
|---------------------------------|----------------------------------------------------------------------------------------|--------------------------------------------------------|--------------------------------------------------------------|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Identify Project | OCIO Project Manager (PM) Departmental client | New IT Project Redesign of existing application | After completion of Project Plan Prior to development | Provide representative to work with OCIO on Project | No role at this point | Work with PM to identify who should be engaged in completing the PPIA |
| Complete Preliminary PIA | PM IP Analyst, OCIO Departmental client rep ATIPP Privacy Analyst | PPIA | Prior to PIA Prior to development | Participate in completing PPIA | Provides guidance towards the completion of the PPIA | Facilitate completion of PPIA Ensure that checklists are completed for all IT projects which require them |
| Evaluate Preliminary PIA | IP Analyst, OCIO (seeks assistance and opinion from ATIPP Office as required) | Sign off PPIA | Prior to development | Ensure that department rep approves of findings of PPIA | Provides advice on “go” or “no go” for PIA Joint Recommendation Letter (OCIO/ATIPP) Maintains copy of PPIA for ATIPP repository | Ensures that PPIAs are completed and signed off Provides copy to ATIPP Office |

| PIA & PPIA Protocol | Who? | What? | When? | Department | ATIPP Office | Information Protection (IP) Analyst, OCIO |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Initiate PIA | <p>Project Manager (creates the Team, in consultation with ATIPP and OCIO IP Analyst)</p> <p>Departmental Client</p> <p>IP Analyst, OCIO</p> <p>ATIPP Office</p> | <p>Form PIA Team</p> <p>Review Preliminary PIA</p> <p>Determine approach</p> | <p>After PPIA indicates that a PIA is required</p> <p>Prior to significant development on system</p> | <p>Provide rep for PIA Team (possibly chair)</p> | <p>Provide expertise; participate as team member</p> | <p>Participate as team member</p> |
| <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> <p>ATIPP Office, OCIO, and Department may collectively decide to outsource PIA at this point</p> </div> | | | | | | |
| Conduct PIA | <p>Project Manager, with support from PIA Team</p> | <p>PIA Template (use PIA Template provided by ATIPP Office)</p> | <p>After formation of PIA Team</p> <p>Prior to significant development</p> | <p>Participate as a member of the PIA Team, provide information as required to facilitate the completion of the PIA</p> | <p>Participate as a member of the PIA Team, provide expertise and support to the PIA Process and Team and to the PM</p> | <p>Participate as a member of the PIA Team; provide expertise and support as required</p> |
| Review PIA | <p>PIA Team, especially</p> <p>OCIO IP Analyst and team member from</p> <p>ATIPP Office</p> | <p>Final review of PIA</p> | <p>After completion of PIA</p> <p>Prior to CIO and Deputy Minister sign off</p> <p>Prior to significant development</p> | <p>Departmental rep agrees with PIA recommendations, as part of PIA Team</p> | <p>ATIPP Office rep on PIA Team agrees with PIA recommendations</p> | <p>IP Analyst, OCIO agrees with PIA recommendations</p> |
| Obtain Sign off | <p>CIO</p> <p>Departmental Client Head (usually DM)</p> | <p>Final sign off on PIA</p> | <p>After agreement on PIA recommendations by PIA Team</p> | <p>Department Head signs off</p> | <p>Maintains a copy of the approved PIA as part of its PIA repository</p> | <p>Ensures that CIO is briefed and obtains CIO signs off on PIA</p> |

Appendix F: Preliminary PIA

Project Name

Contact (Project Manager)

Contact Department or Agency

Contact Title

Contact Email

Contact Telephone Number

Which of the following best describes this project? (Select all that apply)

- Acquisition of commercial application(s) and/or hardware, without significant customization affecting underlying functions (e.g. only customizing the "look and feel" of the application)
- Acquisition of commercial application(s) and/or hardware, with significant customization affecting underlying functions (e.g. customizing data processing, data storage, etc...)
- New development of one or more applications
- Modification or upgrade of one or more existing applications
- Acquisition of IT services from an external vendor
- Acquisition of business services (eg. non-IT services) from an external vendor
- Other (please specify):

Please provide a brief, general description of the project: (attach Project Charter/Plan, if available):

Has this project received formal authority to proceed?

- Yes
- No

If so, where did that authority originate? Attach a copy of the authorization, if available:

Has a PIA been completed for an earlier version of this project or for a substantially similar project?

| | |
|--------------------------|----------------------------------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Not Applicable - this is a new project |
| <input type="checkbox"/> | Unknown |
| <input type="checkbox"/> | Other (please specify): |
| | |

Which departments or agencies of the Government of Newfoundland and Labrador are participating in this project?*

| | |
|--------------------------|-----------------------------------------------------|
| <input type="checkbox"/> | Business |
| <input type="checkbox"/> | Education |
| <input type="checkbox"/> | Environment and Conservation |
| <input type="checkbox"/> | Executive Council |
| <input type="checkbox"/> | <i>Cabinet Secretariat</i> |
| <input type="checkbox"/> | <i>Communications and Consultation</i> |
| <input type="checkbox"/> | <i>Financial Operations Division</i> |
| <input type="checkbox"/> | <i>Office of Protocol</i> |
| <input type="checkbox"/> | <i>Premier's Office</i> |
| <input type="checkbox"/> | <i>Public Service Secretariat</i> |
| <input type="checkbox"/> | <i>Public Service Commission</i> |
| <input type="checkbox"/> | <i>Strategic Human Resource Management Division</i> |
| <input type="checkbox"/> | <i>Transparency and Accountability</i> |
| <input type="checkbox"/> | <i>Intergovernmental Affairs Secretariat</i> |
| <input type="checkbox"/> | <i>Women's Policy Office</i> |
| <input type="checkbox"/> | <i>Rural Secretariat</i> |
| <input type="checkbox"/> | <i>Office of the Chief Information Officer</i> |
| <input type="checkbox"/> | Finance |
| <input type="checkbox"/> | Fisheries and Aquaculture |
| <input type="checkbox"/> | Government Services |
| <input type="checkbox"/> | Health and Community Services |
| <input type="checkbox"/> | Human Resources, Labour and Employment |
| <input type="checkbox"/> | Innovation, Trade and Rural Development |
| <input type="checkbox"/> | Justice |
| <input type="checkbox"/> | Labrador and Aboriginal Affairs |
| <input type="checkbox"/> | Municipal Affairs |
| <input type="checkbox"/> | Natural Resources |

| | |
|--|---------------------------------------------------------------------------------------------------------------------|
| | Tourism, Culture and Recreation |
| | Transportation and Works |
| | Other (including government Agencies and/or any entities outside of the Government of Newfoundland and Labrador): |
| | |

Which departments or agencies of the Government of Newfoundland and Labrador will use or implement the application or service resulting from this project?*

| | |
|--|-----------------------------------------------------|
| | Business |
| | Education |
| | Environment and Conservation |
| | Executive Council |
| | <i>Cabinet Secretariat</i> |
| | <i>Communications and Consultation</i> |
| | <i>Financial Operations Division</i> |
| | <i>Office of Protocol</i> |
| | <i>Premier's Office</i> |
| | <i>Public Service Secretariat</i> |
| | <i>Public Service Commission</i> |
| | <i>Strategic Human Resource Management Division</i> |
| | <i>Transparency and Accountability</i> |
| | <i>Intergovernmental Affairs Secretariat</i> |
| | <i>Women's Policy Office</i> |
| | <i>Rural Secretariat</i> |
| | <i>Office of the Chief Information Officer</i> |
| | Finance |
| | Fisheries and Aquaculture |
| | Government Services |
| | Health and Community Services |
| | Human Resources, Labour and Employment |
| | Innovation, Trade and Rural Development |
| | Justice |
| | Labrador and Aboriginal Affairs |
| | Municipal Affairs |
| | Natural Resources |
| | Tourism, Culture and Recreation |

| | |
|--------------------------|---------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Transportation and Works |
| <input type="checkbox"/> | Other (including government Agencies and/or any entities outside of the Government of Newfoundland and Labrador): |
| <input type="text"/> | |

What is the estimated cost of this project, from inception to completion?

| | |
|--------------------------|-------------------------------------------|
| <input type="checkbox"/> | Less than \$100,000 |
| <input type="checkbox"/> | \$100,000 to \$499,999 |
| <input type="checkbox"/> | \$500,000 to \$1,000,000 |
| <input type="checkbox"/> | More than \$1,000,000 |
| <input type="checkbox"/> | Unknown (please provide further details): |
| <input type="text"/> | |

Has a project plan been submitted to the Office of the Chief Information Officer (OCIO)?

| | |
|--------------------------------------------------------------------|-----|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| If No, indicate if and when a submission will be made to the OCIO: | |
| <input type="text"/> | |

Will the project collect, use or disclose personal information about identifiable individuals?

| | |
|--------------------------|-------------------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Unknown |
| <input type="checkbox"/> | Other (please specify): |
| <input type="text"/> | |

Have you discussed this project's privacy requirements with the OCIO's Information Protection Analyst and/or your departmental Senior Privacy Analyst from the ATIPP Office?

| | |
|--------------------------|----------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Yes - project has been discussed with the OCIO's Information Protection Analyst |
| <input type="checkbox"/> | Yes - project has been discussed with our departmental Senior Privacy Analyst (ATIPP Office) |
| <input type="checkbox"/> | No - project privacy requirements have not been discussed at this time |
| <input type="checkbox"/> | Unknown |
| <input type="checkbox"/> | Please indicate other individuals involved in privacy discussions related to this project: |
| <input type="text"/> | |

Will this project involve outsourcing the collection, use, disclosure, storage or management of personal information?

| | |
|--------------------------|----------------|
| <input type="checkbox"/> | Yes |
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Not Applicable |

| | |
|--|-------------------------|
| | Unknown |
| | Other (please specify): |

What kinds of personal information will be COLLECTED? Check all that apply. (ATIPP S.33(b))

| | |
|--|------------------------------------------------------------------|
| | name |
| | home address |
| | home telephone |
| | email address (non work-related) |
| | race |
| | national origin |
| | ethnic origin |
| | skin colour |
| | religious beliefs |
| | religious associations |
| | political beliefs |
| | political associations |
| | date of birth |
| | age |
| | sex |
| | sexual orientation |
| | marital status |
| | family status |
| | identifying number (eg. SIN, MCP, Drivers License, Employee #) |
| | other identifying particular (eg. Photo) |
| | fingerprints |
| | blood type |
| | inheritable characteristics (eg. DNA) |
| | health care status or history |
| | physical disabilities |
| | mental disabilities |
| | educational status or history |
| | financial status or history |
| | employment status or history |
| | criminal status or history |

| | |
|--------------------------|---------------------------------------------|
| <input type="checkbox"/> | anyone else's opinions about the individual |
| <input type="checkbox"/> | the individual's views or opinions |
| <input type="checkbox"/> | Do not collect personal information |
| <input type="checkbox"/> | Unknown |
| <input type="checkbox"/> | Other (please specify) |
| | |

What kinds of personal information will be USED? Check all that apply. (ATIPP S.38)

| | |
|--------------------------|------------------------------------------------------------------|
| <input type="checkbox"/> | name |
| <input type="checkbox"/> | home address |
| <input type="checkbox"/> | home telephone |
| <input type="checkbox"/> | email address (non work-related) |
| <input type="checkbox"/> | race |
| <input type="checkbox"/> | national origin |
| <input type="checkbox"/> | ethnic origin |
| <input type="checkbox"/> | skin colour |
| <input type="checkbox"/> | religious beliefs |
| <input type="checkbox"/> | religious associations |
| <input type="checkbox"/> | political beliefs |
| <input type="checkbox"/> | political associations |
| <input type="checkbox"/> | date of birth |
| <input type="checkbox"/> | age |
| <input type="checkbox"/> | sex |
| <input type="checkbox"/> | sexual orientation |
| <input type="checkbox"/> | marital status |
| <input type="checkbox"/> | family status |
| <input type="checkbox"/> | identifying number (eg. SIN, MCP, Drivers License, Employee #) |
| <input type="checkbox"/> | other identifying particular (eg. Photo) |
| <input type="checkbox"/> | fingerprints |
| <input type="checkbox"/> | blood type |
| <input type="checkbox"/> | inheritable characteristics (eg. DNA) |
| <input type="checkbox"/> | health care status or history |
| <input type="checkbox"/> | physical disabilities |
| <input type="checkbox"/> | mental disabilities |
| <input type="checkbox"/> | educational status or history |

| | |
|--------------------------|---------------------------------------------|
| <input type="checkbox"/> | financial status or history |
| <input type="checkbox"/> | employment status or history |
| <input type="checkbox"/> | criminal status or history |
| <input type="checkbox"/> | anyone else's opinions about the individual |
| <input type="checkbox"/> | the individual's views or opinions |
| <input type="checkbox"/> | Do not collect personal information |
| <input type="checkbox"/> | Unknown |
| <input type="checkbox"/> | Other (please specify) |

What kinds of personal information will be DISCLOSED? Check all that apply. (ATIPP S.39)

| | |
|--------------------------|------------------------------------------------------------------|
| <input type="checkbox"/> | name |
| <input type="checkbox"/> | home address |
| <input type="checkbox"/> | home telephone |
| <input type="checkbox"/> | email address (non work-related) |
| <input type="checkbox"/> | race |
| <input type="checkbox"/> | national origin |
| <input type="checkbox"/> | ethnic origin |
| <input type="checkbox"/> | skin colour |
| <input type="checkbox"/> | religious beliefs |
| <input type="checkbox"/> | religious associations |
| <input type="checkbox"/> | political beliefs |
| <input type="checkbox"/> | political associations |
| <input type="checkbox"/> | date of birth |
| <input type="checkbox"/> | age |
| <input type="checkbox"/> | sex |
| <input type="checkbox"/> | sexual orientation |
| <input type="checkbox"/> | marital status |
| <input type="checkbox"/> | family status |
| <input type="checkbox"/> | identifying number (eg. SIN, MCP, Drivers License, Employee #) |
| <input type="checkbox"/> | other identifying particular (eg. Photo) |
| <input type="checkbox"/> | fingerprints |
| <input type="checkbox"/> | blood type |
| <input type="checkbox"/> | inheritable characteristics (eg. DNA) |
| <input type="checkbox"/> | health care status or history |

| | |
|--------------------------|---------------------------------------------|
| <input type="checkbox"/> | physical disabilities |
| <input type="checkbox"/> | mental disabilities |
| <input type="checkbox"/> | educational status or history |
| <input type="checkbox"/> | financial status or history |
| <input type="checkbox"/> | employment status or history |
| <input type="checkbox"/> | criminal status or history |
| <input type="checkbox"/> | anyone else's opinions about the individual |
| <input type="checkbox"/> | the individual's views or opinions |
| <input type="checkbox"/> | Do not collect personal information |
| <input type="checkbox"/> | Unknown |
| <input type="checkbox"/> | Other (please specify) |

How will the collection of personal information be authorized? (ATIPP S.32)

| | |
|--------------------------|----------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Expressly authorized by an Act of Newfoundland and Labrador or an Act of Canada |
| <input type="checkbox"/> | Collected for the purposes of law enforcement |
| <input type="checkbox"/> | Information relates directly to and is necessary for an operating program or activity of the public body |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown |
| <input type="checkbox"/> | Other (please specify) |

How will personal information be collected or compiled? (ATIPP S.33)

| | |
|--------------------------|----------------------------------------------------------------|
| <input type="checkbox"/> | Directly from the person who is the subject of the information |
| <input type="checkbox"/> | Directly from a third party |
| <input type="checkbox"/> | Via secondary sources |
| <input type="checkbox"/> | Via data matching |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown / Other (please elaborate below) |

When collecting information directly from the individual, will he or she be: (ATIPP S.33)

| | |
|--------------------------|----------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Informed of the purpose of collection |
| <input type="checkbox"/> | Informed of the legal authority for collection |
| <input type="checkbox"/> | Provided with contact information for a person to whom he or she may address questions |
| <input type="checkbox"/> | Asked to consent to the collection |
| <input type="checkbox"/> | Not Applicable - Do not collect personal information directly from the individual |

| | |
|--|------------------------|
| | Unknown |
| | Other (please specify) |
| | |

If collection is NOT to be directly from the individual, will collection be authorized by any or all of the following: (ATIPP S.33)

| | |
|--|---------------------------|
| | The ATIPP Act |
| | The individual |
| | Another Act or regulation |
| | Not Applicable |
| | Unknown |
| | Other (please specify) |
| | |

Will means be provided to keep personal information accurate, complete and up-to-date as needed for its intended purposes? (ATIPP S.34)

| | |
|--|------------------------|
| | Yes |
| | No |
| | Not Applicable |
| | Unknown |
| | Other (please specify) |
| | |

Will personal information be retained for at least one year? (ATIPP S.37)

| | |
|--|------------------------|
| | Yes |
| | No |
| | Not Applicable |
| | Unknown |
| | Other (please specify) |
| | |

Will individuals be able to request correction of their personal information? (ATIPP S.35)

| | |
|--|------------------------|
| | Yes |
| | No |
| | Not Applicable |
| | Unknown |
| | Other (please specify) |
| | |

Will personal information be protected against such risks as loss or unauthorized access, collection, use, disclosure, destruction, or modification? (ATIPP S.36)

| |
|--------------------------|
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |

- Yes
- No
- Not Applicable
- Unknown

If Yes, please summarize the security measures to be applied:

| |
|--|
| |
|--|

Have you discussed this project with security personnel to address information security measures, or do you intend to do so?

| |
|--------------------------|
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |

- Yes, we have already discussed the project
- Yes, we will discuss the project later
- No
- Not Applicable
- Unknown
- Other (please specify)

| |
|--|
| |
|--|

Will a security assessment (Threat/Risk, Vulnerability) be undertaken?

| |
|--------------------------|
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |

- Yes
- No
- Not Applicable
- Unknown
- Other (please specify)

| |
|--|
| |
|--|

If Yes, please identify the type of assessment: (attach relevant documentation, if available:)

| |
|--|
| |
|--|

Will personal information be used only for purposes consistent with the original purpose of collection? (ATIPP S.38)

| |
|--------------------------|
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |
| <input type="checkbox"/> |

- Yes
- No
- Not Applicable
- Unknown
- Other (please specify)

| |
|--|
| |
|--|

If personal information is used for a purpose other than the original purpose (for which consent was previously obtained), will the individual provide a record of consent for the new use? (ATIPP S.38)

| |
|--------------------------|
| <input type="checkbox"/> |
|--------------------------|

- Yes

| | |
|--------------------------|------------------------|
| <input type="checkbox"/> | No |
| <input type="checkbox"/> | Not Applicable |
| <input type="checkbox"/> | Unknown |
| <input type="checkbox"/> | Other (please specify) |

Will disclosure of personal information be for any of the following purposes identified in the ATIPP Act?

| | |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | To comply with an ATIPP request for access |
| <input type="checkbox"/> | With the individual's consent |
| <input type="checkbox"/> | Consistent with the original purpose of collection |
| <input type="checkbox"/> | To comply with an Act or regulation of the province or of Canada or with a treaty or agreement made under such an enactment |
| <input type="checkbox"/> | When presented with a subpoena, warrant, court order or an order of a person or body with jurisdiction to compel disclosure |
| <input type="checkbox"/> | The information is necessary for a public body employee or Minister in the performance of their duties, or for the protection of their health or safety |
| <input type="checkbox"/> | To the Attorney General for use in civil proceedings involving the government |
| <input type="checkbox"/> | To enforce a legal right that the province or a public body has against any person |
| <input type="checkbox"/> | To collect a fine or debt owed to the public body or the GNL |
| <input type="checkbox"/> | To make a payment owed by the public body or the GNL to any person |
| <input type="checkbox"/> | To the Auditor General or other prescribed person for audit purposes |
| <input type="checkbox"/> | To a member of the House of Assembly who is assisting the individual in the resolution of a problem |
| <input type="checkbox"/> | To a representative of a bargaining agent who is authorized in writing by the subject to make an inquiry |
| <input type="checkbox"/> | To the Provincial Archives of Newfoundland and Labrador or the archives of a public body, for archival purposes |
| <input type="checkbox"/> | To a public body or law enforcement agency for an investigation |
| <input type="checkbox"/> | From one law enforcement agency to another, under terms of a written agreement treaty or legislative authority |
| <input type="checkbox"/> | To contact the next-of-kin or friend of an injured, ill or deceased subject |
| <input type="checkbox"/> | Where compelling circumstances exist that affect a person's health or safety, with notice to the subject |
| <input type="checkbox"/> | In accordance with federal or provincial legislation that authorizes or requires the disclosure |
| <input type="checkbox"/> | For research purposes in accordance with ATIPP S.41 ** |
| <input type="checkbox"/> | By the provincial archives or the archives of a public body under ATIPP S.42 |
| <input type="checkbox"/> | None of the above |
| <input type="checkbox"/> | Not Applicable / No Disclosure |
| <input type="checkbox"/> | Unknown |

Other (please specify)

Please provide any additional comments relevant to this Preliminary Privacy Impact Assessment:

IMPORTANT! Please email this Preliminary PIA Checklist to your departmental Senior Privacy Analyst. If you do not know who your Senior Privacy Analyst is, please contact the ATIPP Office at 729-7072 for assistance.

Appendix G: PIA Template (Annotated)

Privacy Impact Assessment (PIA) Template (Annotated Version)

A Privacy Impact Assessment (PIA) is a formal assessment of the privacy implications within a specific project. This PIA template will guide you through a PIA designed to assess your compliance with the privacy provisions of Newfoundland and Labrador's *Access to Information and Protection of Privacy (ATIPP) Act*.

Note:

The term "project", in this context, is very broad; it refers to a project, program, initiative, legislation, system, application, program, or any other defined course of endeavour.

Under the PIA Policy, public bodies will be required to assess privacy risks for **all** new and significantly redesigned collections, uses and disclosures of personal information that **may give rise to privacy risks**. In order to assess whether a PIA is necessary for your project, please complete a *Preliminary Privacy Impact Assessment (PPIA)*.

Although all Canadian privacy legislation shares common foundations and general principles, this template does not address compliance with any other legislation. If you suspect other privacy legislation may apply, such as the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)*, you should consult your Department's Senior Privacy Analyst in the ATIPP Office.

The annotated version of the template is intended for information purposes only. Please use the electronic version that is not annotated when conducting the actual PIA.

It is important to ensure any deficiencies and issues identified as a result of this exercise are addressed and the necessary adjustments are made within your project. Your Department's Senior Privacy Analyst will be involved in the PIA process and can provide any assistance you require in completing the PIA.

The PIA template is designed to ensure Privacy Impact Assessments consider all relevant factors and issues associated with compliance to the ATIPP Act. The template will walk you through the required information. Before completing the template, complete the following steps:

- 1) Review the Government of Newfoundland and Labrador's *ATIPP Policy and Procedures Manual – Chapter 5*.
- 2) Complete the Preliminary PIA (PPIA), which is documented separately. A completed PPIA should be appended to every completed PIA Template.
- 3) If you are required to complete a different PIA template (e.g. requirement for external funding), please consult the ATIPP Office prior to proceeding.
- 4) Once you determine a PIA is required, assemble the PIA Team and ensure its composition is consistent with the *ATIPP Policy and Procedures Manual – Chapter 5*
- 5) Identify any other legislation that might affect completion of the PIA (e.g. PIPEDA)
- 6) Carefully review this annotated version of the PIA Template and clarify any questions you have regarding its completion. Questions may be directed to your Senior Privacy Analyst.

INSTRUCTIONS

- 1) Have you completed the Project Plan?
- 2) Have you reviewed the *ATIPP Policy and Procedures Manual – Chapter 5*?
- 3) Have you completed the Preliminary PIA?
- 4) Has the Preliminary PIA indicated a PIA is necessary or recommended?
- 5) Have you assembled the PIA team?
- 6) If you have answered “Yes” to the above questions, begin completing the PIA Template.

The PIA Template should not be completed before you have a Project Plan. The Project Plan will provide information and a general context for the completion of the PIA Template. In addition, there is little point in completing a PIA Template until the Project Plan has been approved. Privacy Impact Assessments can involve a significant expenditure of time and effort; therefore, you should know the project is likely to proceed before embarking on a PIA.

Respond to each question by indicating an “X” in the appropriate column (“Yes, No, N/A”) and providing attachments, as required. As often as possible, provide textual answers to the questions in the table. If additional space is required, add further explanations as attachments. Insert the name of the corresponding attachment in the column “Attachments”.

The PIA Template has been designed to be as easy as possible to complete. Most questions can be answered by checking Yes, No or Not Applicable. However, a simple checkmark will often be insufficient to fully respond to the question. The electronic form of the PIA Template will allow you to add text below the question, as necessary. If you need to add larger volumes of text, or if there are existing documents that respond to questions in the Template, you should include them as attachments. Attachments should be clearly marked and cross-referenced. Each attachment should be referenced in the Attachments column with an attachment number and the file name of any related electronic document.

IMPORTANT:

Once submitted, The PIA will likely be a public document. If there is any information that should not be released to the public:

- Attach the information in a separate document
- Clearly mark the information “**Not for Release**”
- Cite the legal authority to not disclose this information

It is very important to remember that the completed PIA is a due diligence exercise and will normally be a public document, available to anyone who requests it, unless there is very good reason to keep information confidential. Such a reason rarely exists for the entire PIA, but may sometimes exist for certain attachments such as information on sensitive security measures. In such cases, any attachments withheld from public release should be separated from all other attachments, clearly marked as “Not for Release” and footnoted with the sections of the access provisions of the ATIPP Act that permit them to be withheld.

PART I - BASIC INFORMATION

| | |
|-----------------------|--|
| Project Name | |
| Date Submitted | |

| | |
|----------------|--|
| Department | |
| Division | |
| Branch/Section | |
| Program | |

Provide the above information in sufficient detail to identify the responsible parties. If there are multiple Departments involved in the project, please complete the above table for each Department, and identify the lead Department for the project.

Contact Information

| | |
|----------------|--|
| Contact Name | |
| Contact Title | |
| Branch/Section | |
| Phone | |
| Email | |

Note:

The Contact identified above should be the individual responsible for completing the PIA Template. This individual should be able to respond to any questions relating to the PIA.

The contact for the PIA Template should be the person who has responsibility for the completion of the PIA. This will likely be the responsible Project Manager, but may in some cases be someone else who has been delegated the responsibility. The contact person should be able to answer any and all questions about the progress of the PIA, or readily obtain answers to such questions.

PART II – DEPARTMENT INFORMATION

Points to Consider

- Each Department should consider having written policies and procedures directing the collection, use, disclosure, and maintenance of personal information
- Include all media of records – paper, electronic documents, audio files, image files, etc. (ATIPP ACT s.2 (q)) and subject to exceptions in s.5(1))

Each part of the PIA Template lists a few points to consider in responding to the questions that follow. In some cases these points will also refer to measures to ensure no undue privacy risks are created.

Questions in Part II relate to the entire Department, not just the project that is the immediate focus of the PIA. The reason for asking questions of this nature is to ascertain whether the Department has the overall privacy practices in place to minimize privacy risks in the long term. If multiple Departments are involved in the project for which the PIA is being undertaken, responses should be provided for all affected Departments, since a privacy failure in any Department could affect the entire project.

| | PART II - DEPARTMENT INFORMATION | Yes | No | N/A | Notes, Attachment References |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 1. | Has the Department provided any privacy management information in a previous PIA? | | | | |
| 2. | If so, has any of this information changed since the previous PIA? If No, please provide the project name and date of the previous PIA. | | | | |
| 3. | Is there an organizational strategic plan or business plan that addresses privacy protection? If Yes, please enclose. | | | | |
| 4. | Does the Department have a written privacy policy? If Yes, please enclose. | | | | |

| | PART II - DEPARTMENT INFORMATION | Yes | No | N/A | Notes, Attachment References |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------------|
| 5. | <p>Has the Department developed privacy guidelines or procedures for its business operations?</p> <p>If Yes, please enclose.</p> <p><i>Such guidelines may address:</i></p> <ul style="list-style-type: none"> <i>a. Right of access to personal information held by government bodies</i> <i>b. Records and Information Management</i> <i>c. Right to request correction of personal information (ATIPP Act s. 35)</i> <i>d. Privacy Breaches</i> <p>See also Part VIII of this PIA Template</p> | | | | |

PART III – PROJECT DESCRIPTION - New or Existing Project

Part III provides a general description of the project in question. If you have documentation already prepared, include it as an attachment. In addition, provide a general description of the project and any explanatory text that may be required for the other questions in this section.

| | PART III - PROJECT DESCRIPTION | Yes | No | N/A | Notes, Attachment References |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | <p>Does the project <u>change</u> an existing program, administrative practice (including contracting to third parties), system or piece of legislation?</p> <p>If Yes, describe the current system or program and the proposed changes. Include the anticipated start date of any changes to current practices.</p> | | | | <p>A Yes or No response without elaboration should be unequivocal; there should be no conditions or qualifications attached to the response. If circumstances are such that neither a firm Yes nor a firm No are possible, attach</p> |
| 2. | <p>Does the project create a new program, administrative practice (including contracting to third parties), system or piece of legislation?</p> <p>If Yes, describe the new system or program and the objectives it is intended to achieve.</p> | | | | |
| 3. | <p>Describe the purpose of the project.</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Provide as much detail as possible in describing the purpose of the project. This can be important in assessing the project's privacy implications, since the ATIPP Act requires the purpose of the project be consistent with the purpose for which any personal information is collected, used or disclosed.</p> </div> | | | | <p>Shaded columns for Yes, No, and N/A indicate that a yes/no response is not appropriate for the question and is therefore not required.</p> |
| 4. | <p>Is this project subject to an Information Sharing Agreement, either within the Government of Newfoundland and Labrador, or between the Government of Newfoundland and Labrador and another government or entity?</p> <p>If Yes, please attach a copy of the agreement and any relevant details.</p> | | | | |

| | PART III - PROJECT DESCRIPTION | Yes | No | N/A | Notes, Attachment References |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| | <p>An Information Sharing Agreement should indicate the authority to collect, use and disclose personal information under legislation, which may include ATIPPA (s. 32 - 42). Such agreements should be in writing and should describe details of the personal information to be shared, as well as the purposes for which the information is to be used. If you have any questions about a given agreement, contact the Office of the ATIPP Coordinator for advice.</p> | | | | |
| <p>5.</p> | <p>Estimate the total cost of this project, from inception to completion?</p> <p><input type="checkbox"/> Less than \$100,000</p> <p><input type="checkbox"/> \$100,000 to \$499,000</p> <p><input type="checkbox"/> \$500,000 to \$1,000,000</p> <p><input type="checkbox"/> more than \$1,000,000</p> <p><input type="checkbox"/> Unknown (please elaborate)</p> <p>The cost of the project provides an indication of its size and scope. All other things being equal, projects with high costs are more likely to involve privacy issues or risks than projects with lower costs.</p> | | | | |
| <p>6.</p> | <p>How many employees (i.e. users) will be directly impacted by this project?</p> <p>How many locations will be affected by this project?</p> <p>The number of employees affected by the project indicates how many employees may have access to personal information that is collected, used or disclosed in connection with the project.</p> | | | | |

| | PART III - PROJECT DESCRIPTION | Yes | No | N/A | Notes, Attachment References |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 7. | <p>Estimate how many records with personal information will be generated in one calendar year.</p> <div data-bbox="355 546 933 622" style="border: 1px solid black; padding: 2px;"> <p>This indicates the volume of personal information involved in the project.</p> </div> | | | | |
| 8. | <p>Estimate how frequently records containing personal information will be accessed in one calendar year?</p> <div data-bbox="355 837 933 913" style="border: 1px solid black; padding: 2px;"> <p>This indicates the extent to which personal information will be used or disclosed.</p> </div> | | | | |
| 9. | <p>Has this project previously been the subject of a Privacy Impact Assessment (PIA) or related review?</p> <p>If Yes, please attach any related documents.</p> <div data-bbox="355 1189 933 1384" style="border: 1px solid black; padding: 2px;"> <p>If the project has previously been the subject of a PIA or related review, it may not be necessary to repeat all responses to the PIA template a second time. When there has been a previous PIA, it is usually sufficient to address those aspects of the project that have changed since the last PIA.</p> </div> | | | | |

| | PART III - PROJECT DESCRIPTION | Yes | No | N/A | Notes, Attachment References |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| <p>10.</p> | <p>Who has been involved in planning the project?</p> <ul style="list-style-type: none"> <input type="checkbox"/> Senior Privacy Analyst (ATIPP) <input type="checkbox"/> Information Protection Analyst (OCIO) <input type="checkbox"/> IT security <input type="checkbox"/> IT systems <input type="checkbox"/> Internal business areas <input type="checkbox"/> External business stakeholders <input type="checkbox"/> Public consultation / involvement (e.g. website feedback) <input type="checkbox"/> <i>Others (specify in notes or attach if necessary)</i> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>Depending on the project, each of these stakeholders may have an important role to play in the assessment of privacy risks and in the implementation of any related mitigation measures.</p> </div> | | | | |
| <p>11.</p> | <p>Briefly describe the types of records (e.g. paper, digital, etc.) and Records Management practices involved in this project.</p> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>Record-keeping practices and records media in Canada have important privacy implications. For example the disposal of paper records containing personal information is often a source of privacy breaches. Similarly, the disposal of computers containing personal information and of backup tapes can be an issue. However, these two issues have quite different solutions, so it is important to know which if any of them apply.</p> </div> | | | | |
| <p>12.</p> | <p>Is personal information being collected, used or disclosed in this project?</p> <p>If No, contact your Senior Privacy Analyst before continuing with this PIA Template.</p> | | | | |

PART IV – PROTECTION OF PERSONAL INFORMATION - SECURITY AND SAFEGUARDS

(ATIPP Act s. 36)

Points to Consider

- For IT- related projects, the Office of the Chief Information Officer (OCIO) will be the lead agency when assessing security and other technical safeguards in this section of the PIA.

Note

Section 36 of the ATIPP Act 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. In addition, internal access to personal information by public employees should be available only on a “need to know” basis, consistent with the purpose for which it was collected.

Information Security and Privacy Protection share several common principles - data quality (accuracy and integrity), data availability, security safeguards, and user limitation (authentication and authorization). Securing data is a key component of protecting personal information. However, it is important to note that some security measures, such as video surveillance, may compromise privacy. It is therefore critical that the privacy implications of a project be considered in the course of the Privacy Impact Assessment. In some cases, the PIA may suggest a need for a Vulnerability Assessment or a more complete security Threat / Risk Assessment, but this is not always the case.

Because the questions in Part IV are general, this section will normally require more than simple Yes/No responses. If a security plan is in place for the project, it should be attached to the PIA. (Note that in some cases the security plan may not be suitable for public release; if so, that should be clearly noted, along with the ATIPP Act provisions that would justify withholding it from release). If there is no security plan or other security documentation, respond to the questions in as much detail as possible.

| | PART IV - SAFEGUARDS AND SECURITY | Yes | No | N/A | Notes, Attachment References |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 1. | <p>Do you have <u>physical</u> safeguards in place to protect against unauthorized access, collection, use, disclosure or disposal of personal information?</p> <p>If Yes, please describe the physical safeguards in place.</p> <div style="border: 1px solid black; padding: 2px; margin-top: 5px;"> <p>Physical safeguards monitor and control the work environment. Physical safeguards may include such things as locks on buildings, doors and cabinets; card access systems; video surveillance and security guards.</p> </div> | | | | |

| | PART IV - SAFEGUARDS AND SECURITY | Yes | No | N/A | Notes, Attachment References |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 2. | <p>Do you have <u>administrative</u> safeguards in place to protect against unauthorized access, collection, use, disclosure or disposal of personal information?</p> <p>If Yes, please attach relevant documentation.</p> <div data-bbox="357 636 935 763" style="border: 1px solid blue; padding: 2px;"> <p>Administrative controls provide a framework for operating and managing the work environment. Administrative controls may include such things as policies, procedures, privacy training, security clearances, etc...</p> </div> <div data-bbox="357 792 935 887" style="border: 1px solid blue; padding: 2px;"> <p>Key policies related to privacy many include such things as security, hiring, disciplinary action, administrative roles and responsibilities, Records and Incident Management.</p> </div> | | | | |
| 3. | <p>Do you have <u>technical</u> security features in place to protect against unauthorized access, collection, use, disclosure or disposal of personal information?</p> <p>If Yes, please describe the technical security features in place to protect personal information.</p> <p>Please attach relevant documentation.</p> <div data-bbox="357 1301 935 1458" style="border: 1px solid blue; padding: 2px;"> <p>Technical or "logical" safeguards monitor and control access to information and computer systems. Technical security features may include such things as user authentication and authorization, passwords, firewalls, data encryption, and network intrusion detection.</p> </div> | | | | |
| 4. | <p>Will this project comply with national and/or international security standards?</p> <p>If Yes, please specify which standards will apply to this project.</p> <div data-bbox="357 1720 935 1883" style="border: 1px solid blue; padding: 2px;"> <p>The ISO 17779 standards can be applied to any project, whereas others, such as the Management of Information Technology Security (MITS), are specific to IT projects. Compliance with one or more security standards will increase the protection around personal information.</p> </div> | | | | |

| | PART IV - SAFEGUARDS AND SECURITY | Yes | No | N/A | Notes, Attachment References |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 5. | <p>Has there been, or will there be, a security Threat and Risk Assessment (TRA) completed for this project?</p> <p>If Yes, please provide details including a copy of the Assessment, if available.</p> <div data-bbox="352 633 936 920" style="border: 1px solid blue; padding: 5px;"> <p>A security Threat and Risk Assessment (TRA) should be completed for any project where personal information is sensitive, collected in large amounts, or disclosed by electronic means. A TRA is especially important for projects involving the electronic transfer of personal information between the Government of Newfoundland and Labrador and third parties other than the subject of the information. Consult the OCIO representative of the PIA team when answering this question.</p> </div> | | | | |
| 6. | <p>If there will be no security Threat and Risk Assessment, will there be a Vulnerability Assessment?</p> <p>If Yes, please provide details including a copy of the assessment if available.</p> <div data-bbox="352 1223 936 1473" style="border: 1px solid blue; padding: 5px;"> <p>Although a security Threat Risk Assessment is preferable, the more limited Vulnerability Assessment may be applied instead. A vulnerability assessment deals with fewer risk factors than a Threat / Risk assessment, but may be appropriate in cases involving specified vulnerabilities, such as malicious intrusions into databases. Consult the OCIO representative on the PIA team before conducting a Vulnerability Assessment.</p> </div> | | | | |

| | PART IV - SAFEGUARDS AND SECURITY | Yes | No | N/A | Notes, Attachment References |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 7. | <p>Have access controls been assigned based on user roles?</p> <p>Access controls are one of the most important security features for the implementation of privacy protection. Access controls are most often implemented in an IT context. Role based access is a good way to ensure that access to personal information is restricted on a need-to-know basis.</p> <p>Access controls can also be implemented in relation to paper records, through restricted access to room or cabinet keys or the use of electronic card keys to implement access controls</p> | | | | |
| 8. | <p>Do controls and procedures exist that govern the authority to add, change or delete personal information?</p> | | | | |
| 9. | <p>Does your system security include an ongoing audit process that can track use of the system (e.g. when and who accessed and updated the system)?</p> <p>If a privacy breach occurs, it is important to be able to track the use of any records or systems that enable access to the affected personal information. In the case of IT systems, this is most commonly implemented through access logs and change logs. For paper-based systems, manual access logs can be used, although they are less reliable than automated logs.</p> | | | | |
| 10. | <p>Please explain the audit process and indicate how frequently audits are undertaken and under what circumstances. Please attach any relevant documentation.</p> <p>Although it is not always necessary, it is considered good practice to periodically review access and change logs (or locks) to assess whether privacy breaches may have occurred. This question asks how such audits are conducted and how often they are scheduled.</p> | | | | |

| | PART IV - SAFEGUARDS AND SECURITY | Yes | No | N/A | Notes, Attachment References |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 11. | <p>Does the audit identify inappropriate access to the system? Please provide details.</p> <div style="border: 1px solid blue; padding: 5px;"> <p>This question relates mostly to IT systems. It asks whether the system generates warnings when inappropriate accesses have occurred, apart from any audit of access logs that may take place. Such warnings may be generated on a case-by-case basis to a system operator, or may take the form of exception reports which are produced periodically. Automated warnings require access logs and user role definitions to function in combination. They can be an effective mechanism for the early identification of potential privacy problems.</p> </div> | | | | |
| 12. | <p>Is there a protocol in place to report and deal with any breach of security affecting personal information? Please provide details.</p> <div style="border: 1px solid blue; padding: 5px;"> <p>The ability to identify breaches of security is of little use if such breaches are not properly dealt with. This question asks whether there is a process in place to escalate real or possible security breaches to those with the related decision-making authority and to ensure that appropriate decisions are taken in a timely manner.</p> </div> | | | | |

IF YOU HAVE ANSWERED 'NO' TO ANY OF THE ABOVE QUESTIONS, PLEASE CONTACT YOUR SENIOR PRIVACY ANALYST FOR ADVICE.

ANY ISSUES RELATED TO SECURITY AND TECHNICAL SAFEGUARDS MUST BE ADDRESSED BY THE OCIO. PLEASE CONTACT THE OCIO IF YOU HAVE ANSWERED 'NO' TO QUESTIONS IN THIS SECTION THAT RELATE TO SECURITY AND TECHNICAL SAFEGUARDS.

IMPORTANT:

A negative response to any of the questions above could indicate a potential security gap with negative ramifications for privacy compliance. Therefore, it is important that any such responses be discussed with your Senior Privacy Analyst and your OCIO representative on the PIA team.

PART V - COLLECTION OF PERSONAL INFORMATION

(ATIPP Act s. 2(o), s. 32 and s. 33)

Points to Consider - Collection of Personal Information

- Personal information is any recorded information about an identifiable individual
- A combination of information can uniquely identify an individual. The pieces of information could be collected at the same time (i.e. *name* and *date of birth*) or from more than one data source (i.e. *data matching*)
- Recognize that this applies to personal information collected by a public body and personal information collected by a third party for a public body (i.e. *contractor*).

| | PART V – COLLECTION OF PERSONAL INFORMATION | Yes | No | N/A | Notes, Attachment References |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 1. | <p>Is personal information being collected?</p> <p>IF NO PERSONAL INFORMATION IS BEING COLLECTED, PROCEED TO “PART VI - USE OF PERSONAL INFORMATION.”</p> <p><i>This question relates specifically to the <u>collection</u> of personal information, as opposed to its use or disclosure. Subsequent sections of the template will address use and disclosure.</i></p> | | | | |
| 2. | <p>What type of personal information will be collected, used and/or disclosed? (E.g. name, home address, gender, Date of Birth, SIN, Employee#, race/nationality, ethnic origin)</p> <p>Please be as detailed as possible.</p> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>It is usually best to attach a list of personal information data elements in response to this question. The list should provide a label and description for each data element, as well as its location in any records or files created or used for the project.</p> </div> | | | | |

| | PART V – COLLECTION OF PERSONAL INFORMATION | Yes | No | N/A | Notes, Attachment References |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 3. | <p>Is personal information collected by a contractor or other external service provider?</p> <p>If Yes, please provide details of the contract or service agreement, especially those provisions addressing privacy protection, confidentiality, and security.</p> <div data-bbox="354 667 935 981" style="border: 1px solid blue; padding: 5px;"> <p>The involvement of contractors or other external service providers in the collection, use or disclosure of personal information can raise particular privacy issues. Under the ATIPP Act, public bodies can contract out various aspects of personal information collection, use and disclosure, but they cannot delegate their responsibilities under the ATIPP Act to the contractor. Consequently, it is critical that contracts and service agreements include provisions to ensure contractors and external service providers exercise the same privacy controls as the public body.</p> </div> | | | | |
| 4. | <p>Describe the manner in which personal information is collected, used or disclosed.</p> <p>Use a table (see example below) or flowchart. Additional diagrams may be necessary in some circumstances.</p> <div data-bbox="354 1261 935 1574" style="border: 1px solid blue; padding: 5px;"> <p>Although this section of the questionnaire deals primarily with data collection, it is often easier to prepare a flowchart or tables showing the collection, use and disclosure of personal information. Often flowcharts will address the flow of each data element individually. However, in some cases that level of detail may not be required, or even appropriate. For example, if a form is described as containing the data elements 'name', 'address', 'phone number,' and 'email' may subsequently be referred to as 'contact information.'</p> </div> | | | | |

Example of Data Elements table:

| Activity | Personal Info | Collected From | When Collected | How Collected | Used By | Disclosed To |
|---------------------------|--------------------------------------------------------------------|-----------------------|--------------------------------|-------------------------|-----------------------------|------------------------------------------------------------------------|
| Moose License Application | Name Address Tel No MCP No Height Eye Colour DOB | Individual | At time of initial application | Submitted by individual | Wildlife Div Science Div | Conservation Officers and Regional District Clerks xwave |

| | PART V – COLLECTION OF PERSONAL INFORMATION | Yes | No | N/A | Notes, Attachment References |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 5. | <p>Is there any data matching between a Department's internal database and any external databases?</p> <p>The term "data matching" refers to the practice of matching records in different databases through the use of a single shared identifier or multiple shared characteristics. Data matching gives rise to specific privacy issues and obligations, since it often involves uses or disclosures that are not consistent with the original purpose of collection. If your project involves data matching, be sure to explain the nature and justification for it in as much detail as possible.</p> <p>Note that data from one or more sources may be non-identifying when considered in isolation, but when it is matched with data from another source the product may include individual identifying data.</p> | | | | |
| 6. | <p>Will the individual be notified of the collection, use, and disclosure of their personal information at the time it is collected? If so, please attach a copy of the notification provided.</p> <p>Such notification may appear in the form of notices on forms, privacy statements on websites, or related information delivered in person or by telephone. Please be as specific as possible in identifying the type of notice an individual will receive and, if available, the wording of that notice.</p> | | | | |

Points to Consider - Authorization for Collection

- Personal information should only be collected when necessary for its intended purposes
- You should be able to demonstrate that any collection of personal information is necessary to meet one of the conditions outlined in the questions below.
- No personal information may be collected by or for a public body unless authorized under the ATIPP Act.

NOTE:

Personal information should not be collected "just in case" it is needed, nor should it be collected under circumstances in which a reasonable person would be surprised by its collection. The ATIPP Act requires authority for any and all collections of personal information.

| | PART V – COLLECTION OF PERSONAL INFORMATION | Yes | No | N/A | Notes, Attachment References |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 7. | <p>Does the purpose of the collection come directly from legislation or regulations (<i>ATIPP Act s.32</i>)?</p> <p>If Yes, cite the relevant section(s) of the legislation in the table provided below.</p> <div style="border: 1px solid blue; padding: 5px;"> <p>Government must have legislative authority for the collection of personal information, whether or not consent has been obtained. Such authority may come from the ATIPP Act or from provisions of related departmental enabling or program legislation. Using the table provided below, list the legislation that gives authority for the collection of personal information in this project:</p> </div> | | | | |
| 8. | <p>Has the collection of personal information been specifically authorized by an Act other than <i>The ATIPP Act (s. 32(a))</i>?</p> <p>If Yes, cite the relevant sections of the legislation in the table below.</p> <div style="border: 1px solid blue; padding: 5px;"> <p>The collection of personal information may be authorized by the general collection provisions of the ATIPP Act (s. 32), or by specific provisions in other legislation. Please cite the Act and section of any legislation that authorizes the collection of personal information for this project.</p> </div> | | | | |

| Legislation | Citation | Short Description | Purpose |
|-------------|----------|-------------------|---------|
| | | | |
| | | | |
| | | | |

IMPORTANT:

*If the purpose for which personal information is collected is not authorized by legislation, **it may not be collected.** Please*

contact your Senior Privacy Analyst before proceeding with the PIA template.

| | PART V - AUTHORIZATION FOR COLLECTION | Yes | No | N/A | Notes, Attachment References |
|-----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 9. | <p>Is the personal information collected for law enforcement purposes?</p> <p>If Yes, specify the law enforcement purpose involved.</p> <div style="border: 1px solid black; padding: 5px;"> <p>The ATIPP Act provides authority for the collection of personal information for law enforcement purposes (s. 32(b)), since law enforcement sometimes requires the collection of personal information in ways that would not be acceptable for other purposes.</p> </div> | | | | |
| 10. | <p>Is the personal information directly related to, and necessary for, an operating program or activity of the public body?</p> <p>If Yes, specify the operating program / activity involved.</p> <div style="border: 1px solid black; padding: 5px;"> <p>If the collection of personal information is not explicitly authorized in legislation or for law enforcement purposes, it must be necessary for the purposes of an operating program or activity (s. 32(c)).</p> </div> | | | | |

IMPORTANT:

If you answered 'No' to Questions 7 – 10 in Part V, this project does not have authority under the ATIPP Act to collect the personal information in question.

Please contact your Senior Privacy Analyst before proceeding with the PIA Template.

Any one of the above questions can provide the necessary authority for the collection of personal information. However, if none of them apply there may be no authority for such collection. If that is the case, it is important to discuss the matter with your Senior Privacy Analyst to determine whether the lack of authority results from an easily corrected oversight, or reflects a more serious deficiency in the proposed project.

Points to Consider – Manner of Collection

- Public bodies should collect only the minimum amount of personal information required to accomplish its purpose
- Personal information may be gathered in a variety of ways, such as interviews, questionnaires, surveys, video recordings, application forms, etc. In completing the PIA template, it is important to review any application forms or other instruments used to collect personal information to ensure they comply with the ATIPP Act
- It is also important to review any written policies and procedures regarding the collection of personal information, and to ensure that all staff members involved in the collection, use or disclosure of personal information receive adequate training so that they are able to comply with the ATIPP Act
- A public body must collect personal information directly from the individual the information is about, with specific exceptions.

| | PART V – MANNER OF COLLECTION | Yes | No | N/A | Notes, Attachment References |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 11. | <p>Will all personal information be collected <u>directly</u> from the individual the information is about?</p> <p>Collection directly from the subject of the personal information is preferable to indirect collection from secondary sources. Direct collection ensures the subject is aware the information has been collected. It also ensures the subject is informed of the purpose for the collection and is given an opportunity to refuse the collection.</p> <p>If you are only collecting personal information <u>directly</u> from the individual, proceed to question V-21, “Notification of Collection”</p> | | | | |
| 12. | <p>If the personal information has not been collected directly from the individual, check which of the following authorizes the indirect collection (s. 33):</p> <p>These questions relate to collection from sources other than the individual the information is about – the ATIPP Act permits such collection only in certain circumstances, as noted in s. 33.</p> | | | | |

| | PART V - MANNER OF COLLECTION | Yes | No | N/A | Notes, Attachment References |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------------|
| 12(a). | Did the individual the information is about authorize or consent to the indirect collection of personal information? (s. 33 (1)(a)(i)) | | | | |
| 12(b). | Has indirect collection been authorized by another act or regulation? (s. 33 (1)(a) (ii)) If yes, please specify the act or regulation and relevant section(s) | | | | |
| 12(c). | Is the personal information being collected for the purpose of determining suitability for an honour or award including an honorary degree, scholarship, prize or bursary? (s.33 (1)(c) (i)) | | | | |
| 12(d). | Is the personal information being collected for the purpose of a proceeding before a court or tribunal? (s.33 (1)(c) (ii)) | | | | |
| 12(e). | Is the personal information being collected for the purpose of collecting a debt, fine or making a payment? (s.33 (1)(c) (iii)) | | | | |
| 12(f). | Is the personal information being collected for the purpose of law enforcement? (s.33 (1)(c) (iv)) | | | | |
| 12(g). | Is the personal information being collected from a third party in the interest of the individual when time or circumstances do not allow collection directly from the individual? (s. 33 (1)(c) (v)) | | | | |
| 12(h). | Is the public body collecting personal information from another public body that is authorized to disclose the personal information under sections 39 – 42 of the ATIPP Act? (s. 33 (1)(b)) Specify relevant section(s) or subsections that apply. Please add additional details as required (e.g., explanation of method of collection) | | | | |

Points to Consider – Notification of Collection

- If information is collected from a third party, it may not be possible to notify the individual the information is about. In such cases, there may be other means of providing a general notification through posters, web sites, or other public displays which explain how and why personal information is being collected.
- A public body must ensure that an individual whose personal information is collected is notified of the collection as outlined in question V-21 below.

| | PART V - NOTIFICATION OF COLLECTION | Yes | No | N/A | Notes, Attachment References |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 13. | <p>Has the individual whose personal information is being collected been informed of:</p> <div style="border: 1px solid blue; padding: 5px; margin: 5px 0;"> <p>Proper notice is an essential element of compliance with the privacy provisions of the ATIPP Act. Be sure that the project includes provisions for notifying individuals whenever their personal information is to be collected.</p> </div> | | | | |
| 13(a). | the purpose for collection?(s. (33(2)(a)) | | | | |
| 13(b). | the authority for the collection? (s. 33(2)(b)) | | | | |
| 13(c). | the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection? (s. 33(2)(c)) | | | | |

IF YOU HAVE NOT PROVIDED THE REQUIRED NOTIFICATION AS OUTLINED ABOVE, PLEASE CONTACT YOUR SENIOR PRIVACY ANALYST.

NOTE:

S. 33 of the ATIPP Act usually requires public bodies to inform individuals from whom they collect information the purpose of the collection, the legal authority for the collection, and a contact number of someone who can answer questions about the collection.

*Section 33 also sets out the circumstances where such notification is not required. **If you answer “YES” to Questions 14 or 15 in Part V, Notification of Collection is not required.***

| | PART V - NOTIFICATION OF COLLECTION | Yes | No | N/A | Notes, Attachment References |
|--------------|------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------------|
| 14. | Is the personal information about law enforcement or anything referred to in the ATIPP Act s. 22(1) or s. 22(2)? | | | | |
| 15. | Has the Head of the Public Body determined that notification would: | | | | |
| 15(a) | Result in the collection of inaccurate information? | | | | |
| 15(b) | Defeat the purpose or prejudice the use for which the personal information is collected? | | | | |

PART VI - USE OF PERSONAL INFORMATION

(ATIPP Act s. 38)

Points to Consider

- Under ATIPPA, a public body must ensure personal information is only used for certain specific purposes as outlined below
- The information should generally only be used for the originally intended purpose.
- S. 38 sets out the situations in which personal information may be used for an additional purpose.

| | PART VI - USE OF PERSONAL INFORMATION | Yes | No | N/A | Notes, Attachment References |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 1(a) | Please provide details of the original purpose for which the personal information was obtained or compiled. | | | | |
| 1(b) | Will the personal information be used only for a use consistent with the original purposes of collection? (Note: "consistent purpose" is defined in the ATIPP Act s. 40) Where applicable, provide details about the consistent purpose and the additional use. | | | | |
| 2. | Has the individual the personal information is about consented to the use? (s. 38(1)(b)) <div style="border: 1px solid blue; padding: 2px;">Although it is not always necessary or even possible, it is preferable to obtain consent from individuals for secondary uses of their personal information if it is feasible to do so.</div> | | | | |
| 3. | If the personal information was initially disclosed for use by a public body under s. 39 - 42 is the information being used for that same purpose? (s.38(1)(c)) Specify subsection(s) being applied. | | | | |

| | PART VI - USE OF PERSONAL INFORMATION | Yes | No | N/A | Notes, Attachment References |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| | | | | | |
| 4. | <p>Is personal information used by a contractor or other external service provider? If Yes, please provide details of the contract or service agreement, especially those provisions addressing privacy protection, confidentiality, and security.</p> <div style="border: 1px solid blue; padding: 5px; margin-top: 10px;"> <p>As noted in the section on collection, special considerations apply when personal information is to be used by a contractor or other external service provider. Be sure to include full details of the uses to which the contractor or service provider will put the data, the conditions attached to such use, and the conditions under which the contractor or external service provider will return the data to the public body or destroy it. Attach copies of the privacy, security, confidentiality and nondisclosure provisions of all related contracts and other service agreements.</p> </div> | | | | |

IF YOU HAVE NOT ANSWERED “YES” TO ANY OF THE QUESTIONS IN PART VI-1 THROUGH VI-3, YOU MAY NOT HAVE AUTHORITY TO USE THE INFORMATION. PLEASE CONTACT YOUR DEPARTMENT’S SENIOR PRIVACY ANALYST BEFORE PROCEEDING.

IF THERE IS NO ADDITIONAL USE OF THE PERSONAL INFORMATION, PROCEED TO PART VII “DISCLOSURE OF PERSONAL INFORMATION.”

PART VII - DISCLOSURE OF PERSONAL INFORMATION

(ATIPP Act s. 39, 40, 41, 42)

Disclosure of Personal Information

- The disclosure of personal information by a public body must be limited to the minimum amount of information necessary to accomplish its purpose.
- **A disclosure of personal information is a release of such information to any organization or individual that is not an employee of the public body that has custody of the personal information.** Note that, for in the ATIPP Act, the word "employee" includes contractors
- Protocols should be in place to educate staff about what to in case of a privacy breach.

IMPORTANT:

A release of personal information from one public body to another is a disclosure, even if both public bodies are departments or agencies of the Government of Newfoundland and Labrador.

| | PART VII - DISCLOSURE OF PERSONAL INFORMATION | Yes | No | N/A | Notes, Attachment References |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 1. | <p>Is personal information being disclosed?</p> <p>Some projects will involve no disclosure of personal information. The personal information involved may be collected and used, but may never be disclosed. If so, potential privacy risks are reduced.</p> | | | | |
| 2. | <p>Is personal information released to a contractor or other external service provider?</p> <p>Is personal information release by a contractor or other external service provider?</p> <p>If yes, please provide details of the contract or service agreement, especially those provisions addressing privacy protection, confidentiality, and security, if those details have not been provided in response to questions above.</p> <p>As noted above, a release of personal information to a contractor is not technically a disclosure, since the contractor is an employee of the public body for ATIPP purposes. The release of personal information to a</p> | | | | |

| | PART VII - DISCLOSURE OF PERSONAL INFORMATION | Yes | No | N/A | Notes, Attachment References |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| | <p>contractor gives rise to particular privacy risks that must be recognized and addressed. Because public bodies cannot delegate their privacy responsibilities to contractors, contractual agreements should bind contractors to an appropriate level of privacy protection.</p> <p>Situations in which contractors disclose personal information to other parties also deserve particular consideration. Such disclosures must always be authorized by the responsible public body, and contractors must disclose personal information only in the same circumstances and with the same care and consideration that the public body would use.</p> | | | | |

IF THERE IS NO PERSONAL INFORMATION BEING DISCLOSED, PROCEED TO PART VIII, “ACCURACY, CORRECTION AND RETENTION OF PERSONAL INFORMATION.”

Authority to Disclose Personal Information

- A public body must ensure personal information in its custody or under its control is disclosed only as permitted under the ATIPP Act s. 39 - 42.
- Please indicate “**Yes**” in the table below to identify the main authorization(s) for disclosure that are applicable:

IMPORTANT:

*All responses to this section should be as detailed as possible. Once information has been disclosed to a third party, the public body and the person the information is about no longer have direct control of that information. For this reason, the Act is most explicit when dealing with disclosure authority. **No disclosure can take place unless it is authorized by one of the provisions in this section.***

| | PART VII – DISCLOSURE OF PERSONAL INFORMATION <i>S.39 (1) AUTHORITY</i> | Yes | No | N/A | Notes, Attachment References |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 3. | <p>Has the consent of the individual the information is about been obtained in the manner set by the minister responsible for this Act?</p> <p>The minister responsible for the ATIPP Act may determine the form and nature of acceptable consent for ATIPP Act purposes. If he or she does so, the relevant regulation must be observed when obtaining consent. If there is no specific consent regulation, the consent should be recorded and in writing.</p> | | | | |

| | PART VII – DISCLOSURE OF PERSONAL INFORMATION <i>S.39 (1) AUTHORITY</i> | Yes | No | N/A | Notes, Attachment References |
|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 4. | Is the information disclosed: | | | | |
| 4a. | for the purpose for which it was obtained or compiled or for a use consistent with that purpose as described in s. 40 | | | | |
| 4b. | for the purpose of complying with an Act or regulation of, or with a treaty, arrangement or agreement made under an Act or regulation of the province or Canada Specify name of Act and relevant section(s) <div style="border: 1px solid blue; padding: 2px;"> It is not enough to simply assert that disclosure is for the purpose of complying with legislation. The specific Act and its relevant provisions must be identified. </div> | | | | |
| 4c. | For the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body with jurisdiction to compel the production of information | | | | |
| 4d | To an officer or employee of the public body or to a minister, where the information is necessary for the performance of the duties, or for the protection of the health or safety of, the officer, employee or minister. <div style="border: 1px solid blue; padding: 2px;"> When relying on this authority, you should specifically and explicitly identify the purpose for which the personal information is required. </div> | | | | |
| 4e. | To the Attorney General for use in civil proceedings involving the government | | | | |
| 4f. | For the purpose of enforcing a legal right the government of the province or a public body has against a person <div style="border: 1px solid blue; padding: 2px;"> Legal advice should be sought before relying on this authority. </div> | | | | |

| | PART VII – DISCLOSURE OF PERSONAL INFORMATION <i>S.39 (1) AUTHORITY</i> | Yes | No | N/A | Notes, Attachment References |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 4g. | For the purpose of: (i) collecting a debt or fine owing by the individual the information is about to the government of the province or to a public body; or (ii) making a payment owing by the government of the province or by a public body to the individual the information is about. | | | | |
| 4h. | To the Auditor General or another person or body described in the regulations for audit purposes <div style="border: 1px solid blue; padding: 2px;"> Personal information may be released to the Auditor General, or to any other entity identified in the regulations, when it is released for audit purposes. </div> | | | | |
| 4i. | To a member of the House of Assembly who has been requested by the individual the information is about to assist in resolving a problem <div style="border: 1px solid blue; padding: 2px;"> Reliance on this authority should be supported by a written request for assistance from the individual to whom the personal information relates. If a written request for assistance is not available, as is sometimes the case, the request from the member should be in writing and should specify that the subject of the personal information as requested his or her assistance. </div> | | | | |
| 4j. | To a representative of a bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry <div style="border: 1px solid blue; padding: 2px;"> A written consent should be required for disclosure under this section. </div> | | | | |
| 4k. | To the Provincial Archives of Newfoundland and Labrador, or the archives of a public body, for archival purposes <div style="border: 1px solid blue; padding: 2px;"> Personal information can be released to the archives as necessary to support its obligation to maintain an archival record of Newfoundland and Labrador. </div> | | | | |

| | PART VII – DISCLOSURE OF PERSONAL INFORMATION <i>S.39 (1) AUTHORITY</i> | Yes | No | N/A | Notes, Attachment References |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 4l. | To a public body or a law enforcement agency in Canada to assist in an investigation: <ul style="list-style-type: none"> (i) undertaken with a view to a law enforcement proceeding; or (ii) From which a law enforcement proceeding is likely to result. | | | | |
| 4m. | Where the public body is a law enforcement agency and the information is disclosed: <ul style="list-style-type: none"> (i) to another law enforcement agency in Canada; or (ii) to a law enforcement agency in a foreign country under an arrangement, written agreement, treaty or legislative authority. | | | | |
| 4n. | Where the head of the public body determines that compelling circumstances exist that affect a person's health or safety and where notice of disclosure is mailed to the last known address of the individual the information is about | | | | |
| 4o. | So that the next of kin or a friend of an injured, ill or deceased individual may be contacted | | | | |
| 4p. | In accordance with an Act of the province or Canada that authorizes or requires the disclosure <div style="border: 1px solid blue; padding: 2px;">Note that federal legislation can authorize or require a disclosure. The <i>Income Tax Act</i> is a prominent example.</div> | | | | |
| 4q. | In accordance with s. 41 and 42. | | | | |

IF YOU HAVE NOT CHECKED ANY OF THE ABOVE AUTHORIZATIONS FOR DISCLOSURE OR REQUIRE CLARIFICATION, YOU SHOULD CONTACT YOUR SENIOR PRIVACY ANALYST.

Disclosure of Personal Information - Research or Statistical Purposes (S. 41)

- Disclosure of personal information for research purposes may only be undertaken if it meets all of the terms set out in section 41 of *the ATIPP Act*.

NOTE:

*Section 41 imposes specific requirements for the handling of personal information to be used for research or statistical purposes. A disclosure under this section will be authorized only if all those conditions have been met. In particular, drafting research agreements requires a thorough understanding of both the privacy implications of the research and the research methodology to be applied. **Contact your Senior Privacy Analyst before assuming that Section 41 can be used to authorize disclosure.***

| | PART VII - DISCLOSURE FOR RESEARCH | Yes | No | N/A | Notes, Attachment References |
|----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 5. | Is there disclosure of non-identifying information for research / statistical purposes? | | | | |
| 6. | Has a researcher requested access to uniquely identifying personal information in an identifiable form for research purposes? If “Yes,” please provide a copy of your research agreement, which should conform to section 41 of the ATIPP Act. If you do not have a research agreement, contact your Senior Privacy Analyst. | | | | |

Disclosure of Personal Information – Archival or Historical Purposes (S. 42)

- The Provincial Archives of the Government of Newfoundland and Labrador, or the archives of a public body, may disclose personal information for archival or historical purposes as authorized by section 42 of *the ATIPP Act*.

NOTE:

The Provincial Archives has the authority to release personal information in its custody or control under specific circumstances, which are addressed in this section. They will apply whenever records created or used in connection with the project being assessed are later released to the Archives at the end of their life cycle.

Please check the applicable authorization(s) for disclosure listed below.

| | PART VII - DISCLOSURE FOR ARCHIVE - S.42 AUTHORITY | Yes | No | N/A | Notes, Attachment References |
|-----|------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 7. | The disclosure is an acceptable disclosure under section 30 | | | | |
| 8. | The disclosure is for historical research and is in compliance with section 41 (research agreements) | | | | |
| 9. | The information is about someone who has been dead for 20 or more years | | | | |
| 10. | The information is in a record that has been in existence for 50 or more years | | | | |

IF YOU HAVE NOT CHECKED ANY OF THE ABOVE AUTHORIZATIONS FOR DISCLOSURE OR REQUIRE CLARIFICATION, PLEASE CONTACT YOUR SENIOR PRIVACY ANALYST BEFORE PROCEEDING WITH THE PIA TEMPLATE.

PART VIII - ACCURACY, CORRECTION, AND RETENTION OF PERSONAL INFORMATION (ATIPP Act S. 34, 35 and 37)

Points to Consider:

Accuracy and Correction of Personal Information

- If an individual's personal information will be used by a public body to make a decision that directly affects that individual, the public body must make every reasonable effort to ensure that the information is accurate and complete (ATIPP Act s.34)
- The ATIPP Act s. 7(1) gives individuals the right to access their own personal information which is in the control or custody of a public body
- The ATIPP Act s. 35 gives individuals the right to have their personal information corrected or annotated and also requires public bodies to notify another public body or third party to whom that information has been disclosed during the one year period before the correction was requested
- For related information, see 'Part II – Question # 5'

Because inaccurate personal information can be harmful to the individual, the maintenance of accurate, up-to-date personal information is a privacy issue when it affects decisions that have an impact on the individual. Procedures referred to in this section should be in writing and should be available to members of the public, on request. Informal procedures that have not yet been put in writing may be referred to here, but the PIA should recommend that they be documented as soon as possible.

| | PART VIII – ACCURACY AND CORRECTION | Yes | No | N/A | Notes, Attachment References |
|----|-------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 1. | Are there procedures in place to enable an individual to request or review a copy of their own personal information? | | | | |
| 2. | Are there procedures in place to correct or annotate an individual's personal information, including the source of the change? | | | | |
| 3. | Are there steps taken to ensure that personal information used to make a decision affecting an individual is accurate and complete? | | | | |
| 4. | Are there steps taken to ensure that an access request is from the individual to whom the information applies? | | | | |

| | PART VIII – ACCURACY AND CORRECTION | Yes | No | N/A | Notes, Attachment References |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 5. | What procedures are in place to allow individuals to correct their personal information? | | | | |
| 6. | What procedures are in place to ensure that personal information can only be modified or corrected by those with the authority to do so? | | | | |
| 7. | If personal information is corrected or annotated, are there procedures in place to notify holders of this information and to ensure all copies of the information in the possession of the public body are corrected / annotated? If Yes, please attach the policy or describe the procedures. | | | | |

IF YOU HAVE ANSWERED “NO” TO ANY OF THE ABOVE QUESTIONS, PLEASE CONTACT YOUR SENIOR PRIVACY ANALYST FOR FURTHER CLARIFICATION.

Points to Consider - Records Management and Retention of Personal Information

- If a public body uses an individual's personal information to make a decision that directly affects the individual, it must retain that information for at least one year after to give the individual a reasonable opportunity to access it (*ATIPP Act s. 37*)
- For related information, see 'Part II - # 5'

| | PART VIII – RECORDS MANAGEMENT AND RETENTION | Yes | No | N/A | Notes, Attachment References |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 1. | Do you have a Records Management policy for records containing personal information? If Yes, please attach the policy. If No, please describe, in detail, current procedures and practices for the collection, use, disclosure and storage of records containing personal information. | | | | |

| | PART VIII – RECORDS MANAGEMENT AND RETENTION | Yes | No | N/A | Notes, Attachment References |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|-----|------------------------------|
| 2. | <p>Do you have physical safeguards in place to protect the storage of records containing personal information?</p> <p>If Yes, please describe the safeguards in place to protect these records.</p> <p>Physical safeguards monitor and control the work environment. Physical safeguards may include such things as locks on buildings, doors and cabinets; card access systems; video surveillance and security guards.</p> | | | | |
| 3. | <p>Do you have a Record Retention and Disposal Schedule for records containing personal information?</p> <p>If Yes, please attach the Schedule.</p> <p>Attach those parts of the Schedule relevant to records of containing personal information. If not specifically referenced, provide a general description.</p> | | | | |
| 4. | <p>If you have a Records Retention and Disposal Schedule, does it ensure information used to make a decision that directly affects an individual is retained for at least one year after use?</p> <p>If no such provision exists in your schedule, the PIA should recommend the insertion of this clause in the schedule.</p> | | | | |
| 5. | <p>Do you have a formalized procedure for the disposal of records containing personal information?</p> <p>If Yes, please provide details.</p> | | | | |

IF YOU ANSWERED "NO" TO ANY OF THE ABOVE QUESTIONS, YOUR PROCEDURES MAY NEED TO BE REVISED. PLEASE CONTACT YOUR SENIOR PRIVACY ANALYST.

Note:

Records of provincial public bodies cannot be destroyed unless approval is granted under the authority of the Rooms Act. Please consult with your records personnel or the Information Protection Analyst (Information Management division) in the Office of the Chief Information Officer for more information.

PART IX – PRIVACY RISKS and RISK MITIGATION STRATEGIES

This is the most important section of the PIA. This section will identify privacy risks in previous sections of the PIA template and discuss measures to mitigate those risks.

- List the responses to PIA questions that suggest possible areas of risk. (They will most often be areas of possible non-compliance with the ATIPP Act, but risks may also arise in areas not explicitly mentioned in the Act, such as in the details of applied security measures.)
- For each response listed, identify the nature of the privacy risk that is raised.

| PIA SECTION | PRIVACY RISKS (cross reference to PIA question) | Probability of Privacy Breach (High, Medium, Low) | Severity of Privacy Breach (High, Medium, Low) | Risk Mitigation Strategy (please include details and rationale)Details and Rationale |
|----------------------|----------------------------------------------------|------------------------------------------------------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Part II - Department | | | | <p>Risks identified in Part II are mainly organizational in nature and relate to the Department's policies and procedures. Risks may include:</p> <ul style="list-style-type: none"> - Inadequate privacy policies - Lack of privacy policies |
| Part III - Project | | | | <p>Risks identified in Part III relate to shortfalls at the project planning stage. Risks may include:</p> <ul style="list-style-type: none"> - Inadequate authority for the project - Inadequate understanding of the project's scope or implications - Failure to consult appropriate parties during the planning process. |

| PIA SECTION | PRIVACY RISKS (cross reference to PIA question) | Probability of Privacy Breach (High, Medium, Low) | Severity of Privacy Breach (High, Medium, Low) | Risk Mitigation Strategy (please include details and rationale)Details and Rationale |
|----------------------------------------|----------------------------------------------------|------------------------------------------------------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Part IV - Information Security risks | | | | <p>As noted in Part IV, inadequate security measures will undermine any privacy measures that may be implemented. Risks may include:</p> <ul style="list-style-type: none"> - Inadequate access controls - Inadequate measures for data integrity - Inability to retrieve information when necessary. |
| Part V – Unauthorized Collection Risks | | | | <p>Risks identified in Part V relate to unauthorized collection of personal information. Risks may include:</p> <ul style="list-style-type: none"> - Collecting personal information without authority - Collecting more personal information than is required |
| Part VI - Risk of unauthorized use | | | | <p>Risks identified in Part VI relate to unauthorized use of personal information. Risks may include:</p> <ul style="list-style-type: none"> - Using personal information for purposes unrelated to the purpose of the original collection - Failing to obtain consent for the use of personal information when it is required - Providing personal information to contractors without adequate controls on their use of the information |

| PIA SECTION | PRIVACY RISKS (cross reference to PIA question) | Probability of Privacy Breach (High, Medium, Low) | Severity of Privacy Breach (High, Medium, Low) | Risk Mitigation Strategy (please include details and rationale)Details and Rationale |
|-----------------------------------------------------|----------------------------------------------------|------------------------------------------------------|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Part VII - Risk of unauthorized disclosure | | | | <p>Because one can never know with certainty where disclosed information has gone after disclosure, the risk of unauthorized disclosure is probably the most important type of risk associated with personal information. Risks may include:</p> <ul style="list-style-type: none"> accidental disclosures to unauthorized persons Susceptibility to deliberate unauthorized disclosure |
| Part VIII - Risk of inaccurate personal information | | | | <p>Because there is a legal obligation to keep personal information as accurate and up-to-date as necessary for its intended purpose, a failure to do so creates a compliance risk. It also poses a risk to the subject of the information, who may suffer detrimental consequences from decisions based on inaccurate, incomplete or out of date personal information.</p> |
| Part XIX - Risk of inadequate records management | | | | <p>Inadequate records management can contribute to any of the above risk classes. For example:</p> <ul style="list-style-type: none"> the unnecessary duplication of personal information can result in problems of inaccuracy if it is not clear which record is the master record. inadequate records management systems can make it difficult to demonstrate privacy compliance even when such compliance has been achieved. |

| PIA SECTION | PRIVACY RISKS (cross reference to PIA question) | Probability of Privacy Breach (High, Medium, Low) | Severity of Privacy Breach (High, Medium, Low) | Risk Mitigation Strategy (please include details and rationale)Details and Rationale |
|-----------------------------------------------------------|----------------------------------------------------|------------------------------------------------------|---------------------------------------------------|--------------------------------------------------------------------------------------|
| <p>Other Risks</p> <p>(add lines as necessary)</p> | | | | |

Privacy Risk Matrix

For each identified risk listed, estimate the likelihood that it will arise in practice and the severity of its consequences for privacy. Assign each risk to the appropriate cell in the matrix. Provide explanatory text, where necessary.

| | Severity of Privacy Risk | | |
|----------------------------|--------------------------|--------|-----|
| Likelihood of Privacy Risk | High | Medium | Low |
| High | | | |
| Medium | | | |
| Low | | | |

Note:

Risks that are classed high in likelihood and severity will be the most important to mitigate quickly and will justify higher mitigation costs. Risks classed low in both dimensions of the matrix may not require immediate mitigation strategies and may not justify high mitigation costs. Most risks will fall somewhere between these two extremes.

The above approach will permit the responsible Deputy Minister(s), as well as the CIO, where appropriate, to evaluate the feasibility of the mitigation measures proposed and the impact of those measures on the project.

IMPORTANT:

Recommendations regarding mitigation measures should be as clear as possible. Some mitigation measures may have implications for the project in areas other than privacy. Such implications may be important to the project sponsors and your recommendations should consider such implications

PART X – PIA TEAM REVIEW

This section ensures the PIA Team has reviewed the PIA and is satisfied with its findings. In projects involving multiple Departments, this section will have to be repeated for each Department involved. The PIA Team should check “Yes” for each question in this section before circulating the PIA for sign off.

| | PART X – PIA Team Review | Yes | No | Additional Information |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|----|------------------------|
| 1. | <p>Does the project meet the requirements of the ATIPP Act? <i>(This question will be answered by the Senior Privacy Analyst)</i></p> <div style="border: 1px solid blue; padding: 2px; margin-top: 5px;"> <p>If the response here is No, be sure to indicate whether recommended mitigation measures will result in full compliance with the ATIPP Act.</p> </div> | | | |
| 2. | <p>Have all PIA Team members reviewed the completed PIA Template and any relevant supporting documentation?</p> <p>Please list all PIA Team members in the “Additional Information” section of this table and indicate which team members, if any, have NOT reviewed the completed PIA.</p> | | | |
| 3. | <p>Do all PIA Team members agree with the privacy risk mitigation recommendations proposed in Section 9 of the PIA Template?</p> <p>If any team member does not agree with the proposed mitigation recommendations, please provide a detailed explanation in the “Additional Information” section of this table.</p> | | | |

PART XI – AUTHORIZATION & APPROVAL

The Project Manager for each Department involved in the project should be responsible for obtaining their Department’s signatures. For projects involving more than one Department, the signature section should be repeated for each Department involved.

Every Department with privacy obligations relating to the project should share in the review and approval of the PIA. For IT projects it may be appropriate for the CIO to sign the PIA before other participating Departments because its acceptance of the PIA will instil greater confidence in other Departments. Alternatively, projects that involve more than one Department sometimes have particularly significant privacy implications for one of the participating Departments. In such cases, that Department should be the first to review the PIA and affix its signatures.

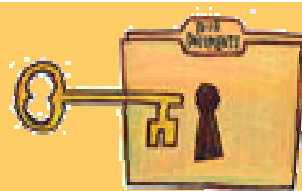
The willingness of signatories to sign off on the PIA should be ascertained before physical signatures are requested. This ensures all outstanding issues are dealt with before the document is ever circulated for signature.

| | |
|----------------------------------------|------|
| Project Manager [Division/Department] | Date |
| Deputy Minister, [Division/Department] | Date |
| Chief Information Officer | Date |

The CIO signature is only required for IT-led projects.

Appendix H: Privacy Breach Protocol

What To Do if a Privacy Breach Occurs



| | |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Know the law | The <i>Access to Information and Protection of Privacy (ATIPP) Act</i> provides individuals a right to access records and a right to privacy protection concerning public bodies in the province of Newfoundland and Labrador. |
| What is privacy? | Privacy can be defined as the right of individuals to control the collection, use and disclosure of personal information about themselves. |
| What is a privacy breach? | A privacy breach occurs when personal information is collected, used, disclosed, retained, or destroyed in a manner inconsistent with the privacy provisions of the ATIPP Act. |
| Who should you notify? | Notify your Manager. You and your Manager will fill out a Privacy Breach Reporting Form and submit it to your department's delegated Privacy Analyst.* |
| Dig deeper | Conduct your investigation using the Key Steps In Responding to a Privacy Breach * |
| Contain the breach | Suspend the process or activity that caused the breach and if possible, get the personal information back into your custody and control immediately. |
| Notification | If necessary, the Breach Notification Assessment Tool will allow you to identify the scope of the breach and determine appropriate notification protocol. The ATIPP Act does not address notification. |
| Prevent future breaches | Take steps to reduce the risk of future breaches (e.g. develop, change or enhance policies and practices). |

Many of the steps outlined above must be carried out simultaneously or in quick succession.

****Please contact the ATIPP Office to obtain the Privacy Breach Reporting Form, Key Steps In Responding to a Privacy Breach, and the Privacy Breach Notification Assessment Tool, or visit us at our website:***

<http://www.justice.gov.nl.ca/just/civil/atipp/>

Privacy Breach Reporting Form

If you are aware of a privacy breach that involves your department or public body, please complete this form and submit it to the Access to Information and Protection of Privacy (ATIPP) Office.

A privacy breach occurs when there is unauthorized collection, use, or disclosure of personal information in contravention of the Access to Information and Protection of Privacy (ATIPP) Act.

The most common privacy breaches involve personal information being lost, stolen, or mistakenly disclosed, such as a laptop containing personal information being stolen or a document with client information being e-mailed to the wrong person.

Please fill out this form in its electronic format (i.e. Microsoft Word). Be sure to complete all sections. You may attach additional pages if necessary. Please indicate if a question does not apply to your situation or if you are not sure how to answer.

Upon completion of this Privacy Breach Reporting Form, please forward via email or fax to your Senior Privacy Analyst in the ATIPP Office. To obtain contact details for your Analyst, please phone the ATIPP Office at 709-729-7072. The Senior Privacy Analyst assigned to your department or public body will contact you upon receipt of this form.

Contact Information

Department / Public Body:

Division / Program:

Contact:

Name:

Title:

Phone:

Fax:

E-Mail:

Mailing address:

Date of Submission to the ATIPP Office:

(Please indicate the date the Privacy Breach Reporting form is completed, not the date in which the privacy breach occurred.)

Risk Evaluation

Incident Description

1. Date the breach occurred:
2. Date the breach was discovered:
3. Describe the breach (provide sufficient detail, including cause):

4. Location of the breach:

5. Estimated number of individuals directly affected by the privacy breach (i.e. whose personal information has been compromised):
6. Type(s) of individuals affected (check all that apply):
 - Client / Customer / Patient
 - Employee
 - Student
 - Other (please specify):
7. Describe any immediate steps taken to reduce the harm of the breach (e.g. retrieval of breached information; replacement of locks; shut down of IT systems, etc...):

Personal Information Involved

8. Describe the personal information involved (e.g. name, address, SIN #, financial information or medical history). ***Do not include or send us the identifiable personal information:***

Safeguards

9. Describe the **physical** safeguards (e.g. locks, alarm systems, etc.) currently in place to protect the personal information in your custody and control:

10. Describe the **administrative** safeguards (policies, procedures, etc...) currently in place to protect the personal information in your custody and control:

11. Describe the **technical** safeguards (access controls, audit controls, etc...) currently in place to protect the personal information in your custody and control:
 - Encryption
 - Password
 - Other (please specify):

Potential Harm

12. Identify any harm that may result from the breach (check all that apply):

- Identify theft (higher risk if breach involves SIN # or financial information)
- physical harm or harassment (e.g. stalking)
- emotional harm, humiliation or damage to reputation (ex. disclosure of mental health records)
- financial cost
- loss of business or employment opportunities
- breach of contract (e.g. from data loss)
- future breaches (technical failures)
- violation of professional standards or certificate standards
- risk to public health or safety
- Other (please specify):

Notification

13. Has your Senior Privacy Analyst in the ATIPP Office been notified?

- Yes Date Analyst was notified:
- No When will the Analyst be notified?

14. Have law enforcement officials been notified?

- Yes Who was notified and when?
- No Will law enforcement be notified at a later time?
 - Yes
 - No

15. Have other authorities (E.g. professional bodies) been contacted?

- Yes Who was notified and when?
- No Will other authorities be notified at a later time?
 - Yes
 - No

Important!

You must contact your Senior Privacy Analyst in the ATIPP Office to discuss notification of individuals affected by the privacy breach. Please review the **Notification Assessment Tool** that is available from the ATIPP Office website:

<http://www.justice.gov.nl.ca/just/civil/atipp/>



Key Steps When Responding to a Privacy Breach

January 2008

This document is for general information only. It is not intended and should not be relied upon as legal or other advice. Its contents do not fetter, bind or constitute a decision or finding by the ATIPP Office with respect to any matter, including any complaint, investigation or other matter. Responsibility for compliance with the ATIPP Act (and any applicable professional or trade standards or requirements) remains with each government department and public body.

**Access to Information and Protection of Privacy Office
Dept. of Justice**

Introduction

Purpose

The purpose of this document is to provide guidance to public bodies and their employees in the occurrence of a privacy breach.

Target Audience

Any public body employee who deals with personal information as part of their work requirement should read this document and be aware of the key steps to be implemented in response to a privacy breach.

What is a Privacy Breach?

A privacy breach occurs when there is unauthorized access, collection, use, disclosure or disposal of personal information. Such activity is “unauthorized” if it occurs in contravention of the *Access to Information and Protection of Privacy (ATIPP) Act*.

The most common privacy breaches occur when personal information of customers, patients, clients or employees is stolen, lost or mistakenly disclosed. For example, a privacy breach occurs when a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong person.

Responding to a Privacy Breach

The most important step you can take is to respond immediately to the breach. You should undertake steps 1, 2 and 3 of this guide immediately following the breach, either simultaneously or in quick succession. Step 4 of this guide provides recommendations for longer-term solutions and prevention strategies.

Contact Information

If you have any questions regarding this document, or privacy in general, please contact us:

Access to Information and Protection of Privacy Office

Department of Justice

4th Floor, East Block, Confederation Building

P.O. Box 8700

St. John's, NL

A1B 4J6

Tel: (709) 729-7072

Fax: (709) 729 -5466

Website: <http://www.justice.gov.nl.ca/just/civil/atipp/>

Step 1: Contain the Breach

You should take immediate actions to contain the breach:

- **Contain the breach** – Immediately stop the unauthorized practice, recover the records, and shut or correct weaknesses in physical security. If the breach is an unauthorized access to an IT asset, such as a computer, server or network, you **MUST** shut down the affected asset and contact the OCIO (or your IT representative) immediately.
- **Immediately contact your Director/Manager** and your delegated Privacy Analyst in the ATIPP Office.
- **Download the *Privacy Breach Reporting Form*** from the Department of Justice website and submit it to your Privacy Analyst.
- If there is criminal harm involved, you should immediately **contact the police or RCMP**.

Step 2: Evaluate the Risks

To determine what other steps are immediately necessary, you should assess the risks associated with the breach. Consider the following factors when assessing the risks:

Personal Information Involved

- What types of information are involved in the breach? Generally, the more sensitive the information, the higher the risk.
- Can the information be used for fraudulent or otherwise harmful purposes? (Social Insurance Numbers and financial information, for example, can be used for identity theft).

Cause and Extent of the Breach

- What is the cause of the breach?
- Is there a risk of ongoing or further exposure of the information?
- How much information was collected, used or disclosed without authorization?
- What is the number of likely recipients?
- Is the information protected by encryption or other means?
- What steps have already been taken to minimize the harm?

Individuals Affected by the Breach

- How many individuals are directly affected by the breach?
- Who was affected by the breach: employees, citizens, clients?

Foreseeable Harm from the Breach

- Is there any relationship between the unauthorized recipients and the information involved in the breach?
- What is the risk of harm to **affected individuals** as a result of the breach?
 - security risk (e.g. physical safety)
 - identity theft or fraud
 - loss of business or employment
 - hurt, humiliation, damage to reputation or relationships
- What is the risk of harm to the **public body** as a result of the breach?
 - loss of trust in the public body or organization
 - loss of assets
 - financial exposure?
- What is the risk of harm to the **general public** as a result of the breach?
 - risk to public health
 - risk to public safety

Step 3: Notification

A key consideration in deciding whether notification is necessary should be the mitigation of harm to any individuals whose personal information has been inappropriately collected, used or disclosed as a result of the breach.

The ATIPP Office has developed a *Privacy Breach Notification Assessment Tool* to assist public bodies in determining when and how to notify individuals. Please contact your Senior Privacy Analyst to obtain a copy of this tool.

Notifying Affected Individuals

As mentioned above, notification of affected individuals should occur if it is necessary to avoid or mitigate harm to them. Some considerations in determining whether to notify individuals affected by the breach include:

- Contractual obligations requiring notification
- Risks of identity theft or fraud (usually due to the type of information lost, such as Social Insurance Number or financial information)
- Physical harm (if the loss puts an individual at risk of being stalked or harassed)
- Risk of hurt, humiliation or damage to reputation (i.e.. disciplinary or medical records being breached)

When and How to Notify

When: If notification is to take place, it should occur as soon as possible following the breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed in order not to impede a criminal investigation.

How: The preferred method of notification is direct (i.e. by phone, letter or in person) to affected individuals. Indirect notification (i.e. website information, posted notices, media) should generally only occur where direct notification could cause further harm, is prohibitive in cost and/or contact information is lacking. Using multiple methods of notification in certain cases may be the most effective approach.

What should be included in the notification?

Notifications should include the following pieces of information:

- Date of the breach
- Description of the breach
- Description of the information inappropriately accessed, collected, used or disclosed
- The steps taken to date to mitigate the harm
- Next steps planned, as well as any long term plans to prevent future breaches
- Advice to the individual to mitigate further harm
- Contact information of an individual within the public body who can answer questions or provide further information
- The right of the individual to complain to the Office of the Information and Privacy Commission (OIPC), noting contact details

Others to Contact

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organizations should also be informed of the breach:

- **Police:** if theft or other crimes are suspected
- **ATIPP Office:** to provide advice or guidance in regard to the privacy breach
- **Insurers or others:** if required by contractual obligations
- **Professional or other regulatory bodies:** if professional or regulatory standards require notification
- **OCIO:** to provide technical and Information Management (IM) advice or guidance in regard to the privacy breach

Step 4: Prevention

Once the immediate steps are taken to mitigate the risks associated with the breach, you should:

- Thoroughly investigate the cause of the breach -- this could require a security audit of both physical and technical security;
- Develop or improve, as necessary, adequate long term safeguards against further breaches;
- Review your policies and update them to reflect the lessons learned from the investigation;
- Audit at the end of the process to ensure that the prevention plan has been fully implemented; and
- Train all staff to know the organization's privacy obligations under the *ATIPP Act*.



Privacy Breach Notification Assessment Tool

January 2008

**Access to Information and Protection of Privacy Office
Department of Justice**

Introduction

The **Access to Information and Protection of Privacy (ATIPP) Office** has created the *Privacy Breach Notification Assessment Tool* to assist you in making key decisions when dealing with a privacy breach.

Public bodies that collect, use and disclose personal information must consider notifying individuals affected by a privacy breach. If a breach occurs as a result of a third party that is under contract with Government, the breach should be reported to the public body, which will be primarily responsible for notification.

The *Privacy Breach Notification Assessment Tool* guides you through four decision-making steps regarding notification in response to a privacy breach:

- **Notifying Affected Individuals**
- **When and How to Notify**
- **What to Include in the Notification**
- **Additional Notifications to Consider**

Contact Information

If you have any questions regarding this document, or privacy in general, please contact us:

Access to Information and Protection of Privacy Office

Department of Justice

4th Floor, East Block, Confederation Building

P.O. Box 8700

St. John's, NL

A1B 4J6

Tel: (709) 729-7072

Fax: (709) 729 -5466

Website: <http://www.justice.gov.nl.ca/just/civil/atipp/>

Notifying Affected Individuals

The following questions will help you decide if notification of affected individuals is recommended. Use your judgment to evaluate the need for notification and if you have any questions, please contact your Senior Privacy Analyst in the ATIPP Office.

| Questions to Consider | Yes | No |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|
| <p>Contractual obligations</p> <p>Do you have a contractual obligation to notify affected individuals in the case of a privacy breach or loss of data?</p> | <input type="checkbox"/> | <input type="checkbox"/> |
| <p>Risk of identity theft</p> <p>Is there a reasonable risk of identity theft or other fraud for affected individuals? Please check all applicable personal identifiers involved in the privacy breach:</p> <p>Social Insurance Number (SIN) <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Driver's License Number <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Medicare Plan Number (MCP) <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Other Identifying Number (Please specify) <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Credit or Debit Card Number <input type="checkbox"/> Yes <input type="checkbox"/> No</p> <p>Other Information that could be used for fraudulent purposes (Please specify) <input type="checkbox"/> Yes <input type="checkbox"/> No</p> | | |
| <p>Risk of physical harm</p> <p>Is there a reasonable risk of physical harm, stalking or harassment for affected individuals?</p> | <input type="checkbox"/> | <input type="checkbox"/> |
| <p>Risk of hurt, humiliation, damage to reputation</p> <p>Is there a reasonable risk of hurt, humiliation or damage to the reputation of affected individuals?</p> <p><i>Risk to reputation may be a concern if the breach includes mental health records, medical records or disciplinary records.</i></p> | <input type="checkbox"/> | <input type="checkbox"/> |

When and How to Notify Affected Individuals

When: Notification should occur as soon as possible following a breach. However, if you have contacted law enforcement authorities, you should determine from those authorities whether notification should be delayed so as not to impede a criminal investigation.

How: The preferred method of notification to affected individuals is direct – by phone, letter or in person. Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost, or is not possible due to lack of contact information..

Multiple methods of notification may be necessary depending on the circumstances surrounding the breach (E.g. the availability of contact information for those affected and the sensitivity of the personal information).

The tables below set out factors to consider in deciding how to notify the affected individuals.

| Considerations Favoring DIRECT Notification | Check if Applicable |
|-------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| The identities of the affected individuals are known | <input type="checkbox"/> |
| Current contact information for the affected individuals can be determined. | <input type="checkbox"/> |
| Affected individuals require detailed information in order to properly protect themselves from harm resulting from the breach | <input type="checkbox"/> |
| Affected individuals may have difficulty understanding an indirect notification (due to mental capacity, age, language, etc.) | <input type="checkbox"/> |
| | <input type="checkbox"/> |

| Considerations Favoring INDIRECT Notification | Check if Applicable |
|-------------------------------------------------------------------------------------------------|----------------------------|
| The number of affected individuals is large such that direct notification could be impractical. | <input type="checkbox"/> |
| Direct notification could compound the harm to the individual resulting from the breach. | <input type="checkbox"/> |

What to Include in the Notification

The information in the notification should help affected individual to reduce or prevent the harm that could be caused by the breach. Include the information set out below:

| Information Required in the Notification | Check if Included |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Date of the breach | <input type="checkbox"/> |
| General description of the breach | <input type="checkbox"/> |
| <p>Description of the information:</p> <p>Provide an overview of the information that was inappropriately accessed, collected, used or disclosed.</p> <p><i>The information should be general and should <u>not</u> include the personal information that was breached. For example, you can say that the individual's Date of Birth was inappropriately disclosed, but you would not state the individual's actual Date of Birth in the notification.</i></p> | <input type="checkbox"/> |
| Steps taken so far to control or reduce the harm | <input type="checkbox"/> |
| Future steps planned to prevent further privacy breaches | <input type="checkbox"/> |
| <p>Steps the individual can take:</p> <p>You should provide information about how individuals can protect themselves in light of the breach (E.g. how to contact credit reporting agencies to set up credit watch, information explaining how to change a personal health number or driver's license number).</p> | <input type="checkbox"/> |
| <p>Organization contact information for further assistance:</p> <p>You should provide contact information for someone within your organization that can answer questions, provide additional information and offer assistance to affected individuals.</p> | <input type="checkbox"/> |
| Information and Privacy Commissioner contact information: | <input type="checkbox"/> |

Additional Notifications to Consider

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider if the following authorities or organizations should also be informed of the breach. Do not share personal information with these other entities unless required.

| Additional Notifications to Consider | Check if Applicable |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <p>Law Enforcement if theft or other crime is suspected</p> <p>Law enforcement may request a temporary delay in notifying individuals for investigative purposes. It is important to discuss these matters with your Privacy Analyst who will assist in seeking legal opinions in the matter of law enforcement.</p> | <input type="checkbox"/> |
| <p>ATIPP Office</p> <p>The ATIPP Office will assist you with developing a procedure for responding to the privacy breach, including notification, and will provide guidance on how to minimize further issues related to the breach.</p> <p>If you have not done so already, you are required to fill out a Privacy Breach Reporting Form, available from the ATIPP Office.</p> | <input type="checkbox"/> |
| <p>Professional or regulatory bodies</p> <p>You should contact the professional or regulatory bodies, if they require notification in such circumstances.</p> | <input type="checkbox"/> |
| <p>OCIO / IT Staff</p> <p>If the breach was a data breach or the result of an information technology failure, you must contact the OCIO or your appropriate IT support staff. Additional contact with third parties may be required to ensure correction or repair of a technical issue.</p> | <input type="checkbox"/> |