

# ATIPP Checklist for Class A Public Bodies

## Purpose

This checklist provides a list of actions and associated resources to help ministerial public bodies implement the Access to Information and Protection of Privacy Act (ATIPP Act).

Class A public bodies, as defined by the [ATIPP Regulations](#), include ministerial public bodies, Yukon University, Yukon Energy Corporation, and Yukon Hospital Corporation. This checklist is relevant for all Class A public bodies because specific information security measures have been prescribed to this category in the ATIPP Regulations.

Resources that are listed below each section are accessible through the [Access to Information Registry](#). Additional information can be found on the Government of Yukon's [Open Government](#) page.

## STATUTORY OFFICERS

---

### Head of Public Body

Has the Head completed the 'Delegation by the Head of the Public Body' form that is provided in the *Toolkit for Heads of Public Bodies*?

Has the delegated individual completed the online training for Heads of Public Bodies?

Has the Head submitted the signed delegation form and provided the name and business contact information of the delegated individual to the ATIPP Office?

Has the delegated individual reviewed the Toolkit for Heads of Public Bodies?

Resources: *Toolkit for Heads of Public Bodies, Delegation by the Head of the Public Body form, ATIPP Act - Training for Ministerial Public Body Heads*

### Designated Officers

#### Designated Access Officer

Has the Head completed the 'Designation of Access Officer by the Head of the Public Body' form to designate one or more employees of a public body to perform the duties and functions of a Designated Access Officer?

Has the signed designation form complete with name and business contact information of the individual(s) been provided to the ATIPP Office?

Has the designated individual(s) completed online training offered through YG Learn?

Level 1: Introduction to the ATIPP Act

Level 2: Access to Information

Has the designated individual(s) reviewed the Designated Access Officer Toolkit and is aware of their responsibilities under Part 3 Access to Information?

Have employees been made aware of who the public body's Designated Access Officers are?

**Resources:** Designation of Access Officer by the Head of the Public Body form; Designated Access Officer Toolkit, ATIPP Act Interpretation Manual; Level 1: Introduction to the ATIPP Act; Level 2: Access to Information; Ministerial Public Body Templates

### Designated Privacy Officer

Has the head completed the 'Designation of Privacy Officer by the Head of the Public Body' form to designate one employee of a public body to perform the duties and functions of a Designated Privacy Officer?

Has the signed designation form complete with name and business contact information of the individual been provided to the ATIPP Office?

Has the designated individual completed online training offered through YG Learn?

Level 1: Introduction to the ATIPP Act

Level 2: Protection of Privacy

Has the individual reviewed the Designated Privacy Officer Toolkit and is aware of their responsibilities under Part 2 Protection of Privacy?

Have employees been made aware of who the public body's Designated Privacy Officers is?

**Resources:** Designation of Privacy Officer by the Head of the Public Body form; Designated Privacy Officer Toolkit, Level 1: Introduction to the ATIPP Act; Level 2: Protection of Privacy; Ministerial Public Body Templates

## Collection, use and disclosure of personal information

### Direct collection of personal information

Collection means to gather or acquire identifiable information about an individual. See also Indirect Collection in the Consent section below for activities related to indirect collection.

Does the public body collect personal information directly from the individual unless it is authorized by the ATIPP Act to collect it from another source? (see Indirect Collection in the Consent section below for activities related to indirect collection)

Does the public body limit the amount of personal information collected to the minimum amount necessary to achieve the purpose for the collection?

Does the public body ensure that personal information will not be collected if non-identifiable information can be used to meet the requirements of the program?

**Resources:** *ATIPP Act, ATIPP Act Interpretation Manual*

## Collection Notices

---

Public bodies that collect personal information directly from an individual must provide a collection notice to the individual in accordance with the ATIPP Act.

Has the public body reviewed collection instruments (forms, public offices with in-take counters) to ensure they meet requirements for collecting personal information?

Do the collection notices provide:

The purpose for collection?

The business contact information of an employee who can answer questions about the collection?

The legal authority for the collection?

Have you established a way to document verbal collection notices with the date of collection? (For example: when notice is provided over the phone) with the date of collection)

**Resources:** *Collection Notice Checklist*

## Unauthorized Collection

---

Public bodies may only collect personal information in accordance with the ATIPP Act and ATIPP Regulations.

Has the public body established a process for employees to report suspected unauthorized collection of personal information?

Do employees (including service providers) know who is the Designated Privacy Officer is?

**Resources:** *Unauthorized Collection Reporting Form for Employees*

## Unauthorized Use

---

Use means to access collected personal information within the department. See the Privacy Breaches section above for activities related to unauthorized use of personal information. See also Indirect Use in the Consent section below for activities related to indirect use.

Does the public body limit the use (access) of personal information to those employees who need to know the information to carry out the purpose for which the information was collected?

Does the public body use non-identifiable or anonymized information instead of personally identifiable information when possible?

Does the public body have a process for ensuring personal information collected is accurate before using it to make a decision?

Does the public body have appropriate safeguards in place to ensure personal information is protected while it is being transmitted and stored for use?

Resources: ATIPP Act, ATIPP Act Interpretation Manual, ATIPP Act Regulations

## Disclosure of personal information

---

Disclosure means to provide access to personal information to anyone outside the department. See the Privacy Breaches section above for activities related to unauthorized disclosure of personal information.

Does the public body limit the disclosure of personal information to the minimum amount necessary to accomplish the purpose for which it is to be disclosed?

Does the public body disclose non-identifiable or anonymized information instead of personally identifiable information when possible?

Does the public body have appropriate safeguards in place to ensure personal information is protected while it is being transmitted for disclosure?

Does the public body have appropriate Agreements in place with third parties to ensure the protection of personal information being disclosed (See Agreements section above for activities related to Agreements)

Resources: ATIPP Act, ATIPP Act Interpretation Manual, ATIPP Act Regulations, Information Sharing Agreement Guidance; Information Sharing Agreement Template; Information Sharing Agreement Tracking Log; Research Agreement Proposal Template; Research Agreement Notification Template; Agreement for Access to Personal Information for Research or Statistical Purposes Template

## Consent

---

Indirect collection, use and disclosure of personal information may be authorized if an individual consents in the prescribed manner.

### Indirect Collection with Consent

When the public body indirectly collects personal information from another source, does the individual provide voluntary consent?

Do consent forms indicate the specific type or class of personal information to be indirectly collected?

Do consent forms state the purpose for and the source of indirect collection?

Does the public body have a process for ensuring personal information indirectly collected is accurate?

When consent for indirect collection of an individual's name, addresses, including electronic addresses, and phone numbers is provided orally, is a written record of the consent produced?

Is there a time period specified for the consent? Is an expiration date supplied or will the information only be used until the purpose has been fulfilled?

Does the public body retain the written record of the consent for indirect collection for as long as the public body relies on the consent and a period of one year afterwards?

**Resources: ATIPP Act Regulations**

### Use with Consent

Do the terms of consent set out the purpose for which the personal information may be used if the use is for a different purpose from the purpose for which it was collected?

Do consent forms indicate the specific type or class of personal information to be used?

Does the public body have appropriate safeguards in place to ensure personal information is protected while it is being transmitted for use?

### Disclosure with Consent

Do the terms of consent set out the purpose for which the personal information may be disclosed if the disclosure is for a different purpose from the purpose for which it was collected?

Do consent forms indicate the specific type or class of personal information to be disclosed?

Do consent forms state to whom the personal information will be disclosed to?

Does the public body have appropriate safeguards in place to ensure indirectly collected personal information is protected while it is being transmitted for disclosure?

Does the public body have appropriate Agreements in place with third parties to ensure the protection of indirectly collected personal information being disclosed (See Agreements section above for activities related to Agreements)

*Resources: ATIPP Act Regulations, Information Sharing Agreement Guidance; Information Sharing Agreement Template; Information Sharing Agreement Tracking Log; Research Agreement Proposal Template; Research Agreement Notification Template; Agreement for Access to Personal*

## Withdrawal of Consent

Does the public body have a process to accept and approve requests for withdrawal of consent for indirect collection of personal information?

Does the department create a written record to document withdrawal of consent for the period of one year after the effective date of withdrawal of consent?

*Resources: ATIPP Act Regulations*

## Access Requests

### Formal Access Requests (administered through the ATIPP Office)

Have employees been made aware of their responsibility under the ATIPP Act to respond to a request for records from the Designated Access Officer and associated timeline for response?

### Informal Access Requests (direct requests from the public)

Does the public body have established procedures for informal access requests of information from the public?

Are employees aware of what can and cannot be released informally?

Have employees been made aware of who the public body's Designated Officers are to ask questions regarding an informal access request?

*Resources: Designated Access Officer Toolkit*

## Agreements

---

Agreements provide a formal administrative mechanism to solidify an understanding between parties to establish terms and conditions by which information is shared and protected.

Is this an agreement (contract, transfer payment or other agreement) that involves the management and safeguarding of personal information through a third-party service provider?

Has the public body identified all parties to which it shares (including disclosure) information to?

Has the public body entered into formal Information Sharing Agreements (ISA) with these parties?

Has the public body entered into formal Research Agreements if sharing personal information with a Researcher, for a research purpose?

Has the public body identified Information Managers engaged by the organization, and if so has it entered into Information Manager Service Agreements (IMSA) with these parties?

Do any applicable Agreements contain requirements from the ATIPP Act and ATIPP Act Regulations, including clauses that specify:

Who is accountable for complying with the agreement?

The purpose of the agreement and what types of information will be collected, used and disclosed, including any limitations or conditions?

The authorities for collection, use and disclosure of information?

How retention and disposal of personal information will occur?

The effective date of the agreement and how termination may occur?

**Resources:** *Information Sharing Agreement Guidance; Information Sharing Agreement Template; Information Sharing Agreement Tracking Log; Research Agreement Proposal Template; Research Agreement Notification Template; Agreement for Access to Personal Information for Research or Statistical Purposes Template*

## Security of Information

---

Public bodies must establish and implement administrative, technical and physical security measures to protect personal information of each type or class of personal information that it holds.

Does the public body follow standard written guidelines for privacy breaches that sets out the responsibilities of employees, Designated Privacy Officers and Heads?

Does the public body have security measures to protect personal information against risks of:

- Inadvertent or authorized modification?
- Damage, corruption or unintended destruction?
- To prevent information from becoming inaccessible?
- To prevent unsecured storage, transmittal or transfer?
- To prevent theft, loss, unauthorized use, disclosure or disposal?
- To prevent any other threat or hazard that may exist?

Does the public body conduct a Security Threat Risk Assessment (STRA) before carrying out:

- A proposed or significant change to a personal identity service?
- A proposed or significant change to an integrated service?
- A proposed or significant change to a data-linking activity?
- A proposed or significant change to an information management service?
- Does the public body provide a copy of the STRAs relating to these initiatives with the Office of the Information and Privacy Commissioner (OIPC)?
- Do the public body's electronic information systems provide a record of user activity for each user who accesses personal information?

Does the public body have written policies for protecting personal information holdings that include how the public body:

- Periodically tests and evaluates security measures;
- Modifies or updates security measures as required to comply with the ATIPP Act Regulations;
- Speaks to the security strategy to establish and implement security measures;

Designates an employee to:

- Provide training to employees;
- Monitor compliance; and
- Respond to inquiries.

**Resources: ATIPP Act Regulations**



# Protection of Privacy

## Privacy Breaches

---

Privacy breach”, in respect of personal information, means the theft or loss of, or unauthorized use, disclosure or disposal of, the personal information.

Has the public body established a written process for receiving and responding to reports of suspected privacy breaches of personal information from both members of the public and employees?

Have employees been trained to identify a suspected breach and their requirement under the ATIPP Act to report their suspicions without delay, to the public body's Designated Privacy Officer?

Does the public body have a process to ensure notification when necessary to an individual affected by a privacy breach?

Does the public body have a process to ensure notification when necessary to the ATIPP Office and Office of the Information and Privacy Commissioner (OIPC)?

Does the public body maintain a written record of suspected and confirmed breaches to identify trends and training opportunities for employees?

**Resources:** *Designated Privacy Officer Toolkit; Privacy Breach Reporting Form for Employees; Designated Privacy Officer Breach Reporting Form; Privacy Breach Notification Template, Privacy Breach Protocol*

## Correction Requests

---

An individual who believes that there is an error or omission related to any of their personal information may request that the Head of the public body correct the error or omission.

Does the public body have a written policy for responding to and making decisions about personal information correction requests?

Does the public body have a procedure for correcting or annotating a paper or electronic record when a correction to personal information is to be made?

Does the written policy include a process for notifying other public bodies or agencies that the personal information has been shared with, to correct or annotate their records?

**Resources:** *ATIPP Act Regulations*

## Privacy Impact Assessments

---

A Privacy Impact Assessment (PIA) is a process for evaluating a proposal in terms of its impact on privacy. It identifies potential effects, privacy risks and suggests approaches for mitigation.

Does the public body ensure that a PIA is undertaken when proposing a new program/activity or significant change to an existing program/activity?

Does the public body ensure that a PIA is undertaken when proposing or making a significant change an information management service?

Has a copy of the completed PIA been provided to the ATIPP Office?

When the public body is proposing or making a significant change to a specialized service (integrated service or personal identity service):

Has a copy of the completed PIA been provided to the ATIPP Office?

Has the OIPC been consulted?

Has the drafting of a regulation been initiated under section 27 or 28 of the ATIPP Act?

Has the draft PIA been provided to the OIPC for recommendations 30 days prior to implementation?

Has the public body responded to the OIPC recommendations?

Has the completed PIA been provided to the ATIPP Office?

When the public body is proposing or making a significant change to a data-linking activity:

Has the OIPC been consulted?

Has the drafting of a regulation been initiated under section 29 of the ATIPP Act?

Has the draft PIA been provided to the OIPC for recommendations 30 days prior to implementation?

Has the public body responded to the OIPC recommendations?

Has the completed PIA been provided to the ATIPP Office?

**Resources:** *Privacy Impact Assessment Toolkit; Privacy and Security Assessment; Privacy Impact Assessment Template Schedule A; Privacy Impact Assessment Schedule B; Privacy Impact Assessment Schedule D*