Guidance for Public Bodies on Accountable Privacy Management

January 29, 2015

Table of Contents

Acknowledgements

This guidance was developed from materials created by the Office of the Information and Privacy Commissioner for British Columbia (OIPC BC) and similar resources developed by the OIPC BC in conjunction with the Office of the Information and Privacy Commissioner of Alberta and the Office of the Privacy Commissioner of Canada. We wish to recognize these offices for their work and to thank the OIPC BC for permission to utilize their Accountable Privacy Management in BC's Public Sector guidance as the basis for developing this guidance.

Purpose and Explanatory Notes

This document provides step-by-step guidance for Yukon's public bodies on how to implement an effective privacy management program.

The Office of Yukon's Information and Privacy Commissioner (OIPC) intends to use this document in its investigative and compliance review work. As part of this work the OIPC will be looking for evidence of a public body's privacy management program.

Part A of this document outlines the fundamentals of a privacy management program. Part B outlines how a public body can ensure their privacy management program is effective.[1]

This document does not provide legal or other advice. It does not affect the powers, duties or functions of Yukon's Information and Privacy Commissioner (IPC) or the rest of the OIPC respecting any complaint, investigation or other matter under or connected with the IPC's authority under the *Access to Information and Protection of Privacy Act* (ATIPP Act) and the matters addressed in this document.

[1] The appendix to this document offers links to privacy compliance resources prepared by Privacy Commissioners' offices, including resources from the OIPC, dealing with different aspects of privacy compliance. These resources may further assist public bodies design and implement their privacy management programs.

Definitions

Personal information, as defined in the ATIPP Act, means "recorded information about an identifiable individual."

Privacy means the protection of personal information by a public body in accordance with the ATIPP Act.

Public body means a body under the ATIPP Act that is required to comply with the ATIPP Act for records in its custody or control.

Introduction

As public bodies seek to serve Yukoners in innovative ways, they are looking for efficiencies in how they design and deliver services and for new approaches to old problems. Analyzing personal information is an increasingly critical part of these efforts. It is also key to public bodies gaining a better understanding of Yukoners' needs. More and more public bodies are using electronic personal information and analytic technologies to achieve these purposes.

Public bodies have the power to compel Yukoners to give up their personal information in ways that businesses cannot and in doing so significantly impact on their privacy. Yukoners have a choice about whether to conduct business with a private sector business. They do not generally have a choice whether to conduct business with government. Given this, public bodies must ensure they are effectively meeting their legal obligations to protect Yukoners' privacy.

This is the context and reason for this document which aims to guide Yukon's public bodies on what it means to be accountable for privacy and what the OIPC expects a public body to have in place to effectively manage its legal obligations under the ATIPP Act.

What is accountability?

Accountability in relation to privacy means a public body's acceptance of its responsibility to protect privacy in accordance with its legal obligations. In order to demonstrate accountability for protecting privacy, a public body must be able to demonstrate the existence of a privacy management program.

A privacy management program ensures that privacy is built into all initiatives, programs or services by design. Responsible management of privacy is critical to build and maintain the trust of Yukoners, who are increasingly concerned about the effect of new and emerging technologies on privacy, especially digital solutions for managing personal information.

As the volume, type and sensitivity of personal information in the custody or control of a public body will vary, a privacy management program must be adapted to the unique needs of each public body. This document provides a scalable framework all public bodies can use.

While the concept of accountability may appear to be straightforward, creating a privacy management program requires thoughtful planning to ensure its effectiveness within a public body. Public bodies need to design and implement a practical, effective and properly-resourced privacy management program that is consistent with the principles outlined in this document and the provisions of the ATIPP Act.

Steps for setting up the program

Prior to designing a privacy management program, a public body should first assess its existing approaches to privacy compliance. To do this, it should follow the steps below:

1. Appoint a project lead with sufficient privacy knowledge and authority to manage the project and assess the findings (this could be a privacy officer, discussed below).

2. Ensure there is oversight by executive management.

3. To the extent necessary involve human resources, risk management, policy, internal audit, and information communications technology (ICT) personnel.

4. Obtain outside privacy program development expertise if necessary.

5. Obtain and document the information necessary to assess compliance. This information may be obtained through policy review, staff interviews, file reviews, and ICT system reviews;

6. Ensure executive management receives regular reports on progress and any direction provided is implemented.

7. Report any risks associated with non-compliance to executive management.

8. Provide a final report of the findings to executive management with a full mapping of the findings against the ATIPP Act's requirements.[2]

9. Complete any other steps that might, in light of the public body's own situation, be desirable to document its current state of compliance and the way forward.[3]

[2] Some public bodies may be subject to other legislated privacy requirements that need to be taken into account when developing a privacy management program.

[3] These factors are consistent with the 'AICA/CICA Privacy Maturity Model' (March 2011), found at: http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/docs/item48094.pdf.

A. Privacy Management Program Essentials

This part describes the fundamental privacy management program building blocks that every Yukon public body must have in place in order to meet their legal obligation to protect privacy under the ATIPP Act. It is not possible, of course, to describe a universally-applicable approach. For one thing, public bodies vary in size, mandate and functions, and the kinds of personal information they collect and what they do with it vary widely. The guidance is intended to be scalable to fit the unique needs of public bodies who work through these building blocks.

1) Demonstrating Commitment to Privacy Compliance

The first building block involves the development of a robust and well-thought-out internal governance structure that prioritizes privacy compliance and fosters a privacy-respectful culture. This building block recognizes that more is needed than policies and procedures to give effect to the ATIPP Act's requirements to protect privacy. Public bodies need to create and maintain a culture of privacy awareness in order to ensure that privacy issues are recognized and addressed as they arise. Building a culture of privacy awareness is a key component of accountability for privacy protection.

a) Demonstrating senior management commitment and support

Executive management support is at the heart of a privacy-respectful culture and of any successful privacy management program. Executive management's commitment to compliance with the ATIPP Act coupled with the other building blocks increase the likelihood that the public body's privacy management program will succeed. Executive management's commitment is, therefore, a necessary component of a privacy management program.

To actively champion a privacy management program, executive management needs to ensure that the resources necessary to develop, implement, assess and revise the program are available. Public bodies face competing demands for public resources, which can be scarce. However, given that individuals essentially have no choice in providing their personal information to a public body means that compliance with the ATIPP Act should be among those priorities. Being able to demonstrate the ability to comply with the ATIPP Act by having a properly resourced privacy management program will reassure citizens that the public body is able meet these obligations when using citizens' personal information to achieve its objectives.

b) Designate and empower a Privacy Officer

Executive management should designate a person, such as a privacy officer, to be responsible for ensuring the public body's compliance with the ATIPP Act and who is also responsible for the management and direction of the privacy management program.[4] Executive management should also ensure the program is adequately resourced.

Adequacy of program resources is important. In smaller public bodies, such as many Yukon departments, the privacy officer may be able to assume other duties without affecting the ability to discharge privacy compliance duties. In larger public bodies, or those that manage a significant amount of highly sensitive personal information and use a number of electronic databases to conduct business, it is much more likely that the privacy officer will not be able to perform other duties without negatively affecting privacy protection. In these public bodies, a privacy officer may also need support staff.

It is important that executive management assess the resources needed by the public body to ensure legislative compliance and good practice. This can be done as part of the initial assessment and design of the privacy management program, with appropriate resources and staff being dedicated to carrying it out once the program is approved for implementation. To determine the resources, the role of privacy officer should be taken into account.

The role of privacy officer must be clearly defined and positioned within the public body such that they form part of the public body's decision making processes. In establishing a privacy management program, the role of the privacy officer is to:

- develop the program controls,
- identify the resources required for effective management of the program,
- implement the program controls, which involves training, incorporating the controls into existing business processes, and communicating its existence and purpose widely within the public body,
- assess the effectiveness of the program, which involves staying abreast of the privacy law landscape and threats to privacy both from within and external to the public body, and
- revise the program as necessary to ensure its effectiveness.

Annual budgets for a privacy management program should reflect shifting needs for compliance resources, including those driven by changes to legislation; public body administration and management; new programs involving personal information and outsourcing of services; or the new use of electronic systems or integrated systems for collecting, using or disclosing personal information.

[4] Public bodies must keep in mind that designation of a Privacy Officer does not diminish their ultimate accountability for compliance with ATIPP.

c) Compliance reporting

Executive management should establish reporting mechanisms to be kept informed, through the privacy officer, about whether the program is functioning as expected, how and why it is not, and of the proposed fixes. Breach reporting should be included among reporting requirements to ensure executive management is notified about privacy breaches and to provide any direction for management of the breach. Breach and complaints management should be centralized with the privacy officer in order to facilitate this reporting.

Mechanisms designed to facilitate reporting must clearly define when and how a matter is to be escalated, and to whom. It may be useful to evaluate the robustness of the escalation and reporting process by conducting a test run of, especially, privacy breach management processes, to ensure effective reporting occurs.

2) Program Controls

The second building block involves the development of program controls. Program controls are those controls utilized as part of a privacy management program to effectively manage compliance requirements. Program controls consist of a personal information inventory, policies and procedures, risk assessment tools, training, breach and incident management, service provider management, and communicating with individuals.

a) Personal information inventory

If a public body does not know, to a reasonable degree of specificity, the nature and amount of personal information it is collecting, using, disclosing and retaining and the purposes and conditions for those activities, it will be unable to ensure the information is managed in accordance with the ATIPP Act. Therefore, having a personal information inventory is an essential component of a privacy management program.

Public bodies will want to ensure their inventory covers only personal information as the ATIPP Act defines it. "Personal information" is defined in the ATIPP Act as "recorded information about an identifiable individual". If a public body is not sure whether it is collecting "information about an identifiable individual", it should keep in mind that the definition should be interpreted in a remedial way and shall be given a fair, large and liberal interpretation that best insures the attainment of the objects of the ATIPP Act.[5] Generally speaking, if information either identifies an individual (including through a unique identifier) or the information could, when combined with other available information, reasonably identify an individual and the information is about the individual the information will be personal information. In cases of doubt, the public body should seek legal advice on the issue.

[5] *Interpretation Act*, RSY 2002, c.125, section 10.

Public bodies will also want to ensure their inventory covers information that is in the custody and control of the public body which could include personal information collected, used or disclosed under a service provider relationship. The ATIPP Act applies only to records that are in the custody or under the control of the public body.[6]

A personal information inventory should include the following elements:

- amount and categories of personal information;
- number and categories of individuals whose personal information it holds;
- location where personal information is held, both within the public body and where it is held by third parties (including service providers);
- purposes for which personal information is collected, used and disclosed; and
- sensitivity of the personal information the public body holds.

b) Privacy policies and procedures

Policies and procedures establish the rules employees of a public body are required to follow to protect the privacy of personal information in the custody or under the control of a public body. Without privacy policies and procedures, a public body's ATIPP Act compliance will be *ad hoc* and potentially haphazard. Therefore, having written policies and procedures setting out these rules for employees are an essential component of a privacy management program.

Policies and procedures should include:

- the purpose and authority for collection, use and disclosure of personal information;
- requirements for notification and consent;
- how to ensure accuracy of personal information;
- how to facilitate access to and correction of personal information;
- retention and destruction or disposal of personal information;
- how personal information will be secured;
- how a privacy breach will be managed; and
- how complaints will be managed.

Policies should address all aspects of managing personal information and related privacy obligations.

A review of other policies should be undertaken to evaluate any impact on privacy. Policies in relation to contract management, procurement, human resources, research, disclosure of personal information to other public bodies, regulatory bodies and law enforcement agencies may, for example, need to be revised.

[6] ATIPP Act, RSY 2002, c.1, section 2.

The next section discusses each of the above key policies in more detail.

i. *Authority for collection, use and disclosure of personal information*

The policy needs to identify the personal information the public body is authorized to collect, the purpose of collection, use and disclosure and authority under the ATIPP Act. The policy should also address when and how the public body may collect personal information indirectly (from someone other than the individual the information is about) and the authority for indirect collection.

ii. *Requirements for consent and notification*

The policy will need to address if the public body is required to give notice about the collection of personal information, and if required how notice will be given and its contents. If consent is identified as the authority to use and disclose personal information in the policy, the method of obtaining consent and the contents should be included.

iii. *Accuracy of personal information*

The policy will need to address how the public body will ensure the accuracy of personal information where it plans to use personal information to make a decision directly affecting an individual.[7] The policy should also address how the public body will ensure the information is kept up to date.

iv. *Access to and correction of personal information*

The policy will need to specify the process for providing access to and correction of personal information. Under the ATIPP Act, formal requests for access and correction are to be processed through the Records Manager. However, public bodies may choose to make personal information accessible to individuals or make corrections without requiring the individual go through the formal process. If a public body chooses to do so, it should specify in policy how that process will operate and where centralized, for example with the privacy officer, the position responsible for processing these requests.

v. *Retention and disposal of personal information*

The policy will need to address the retention of personal information. A public body should only retain personal information as long as is required to meet business and legal requirements. The ATIPP Act requires a public body to retain personal information for at least one year after it is used to make any decision that directly affects the individual the information is about.[8]

[7] ATIPP Act, RSY 2002, c.1, section 31.
[8] ATIPP Act, RSY 2002, c.1, section 34.

Part of determining retention requires a public body to specify a disposal or destruction date, or for records of archival value the date of transfer to the archives. Any records management policies and procedures that exist in the public body should be referred to for these dates.

Retention of personal information beyond what is required for a business or legal purpose is not recommended as doing so increases the risks to the security of the personal information.

vi. *Security of personal information*

The policy will need to address how the public body will meet its obligation to secure the personal information by making reasonable security arrangements against such risks as accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal.[9] What is reasonable depends on the sensitivity of the information and a variety of other factors including whether the personal information is electronic and the number of employees with access to it. The policy should detail the administrative, technical and physical controls required to properly secure personal information.

Administrative controls are rules about things like responsible use of technology, use of agreements acknowledging privacy responsibilities, granting access to personal information (electronic or paper), role based access (see below), transmission of information (such as by internet, fax, email, mail or courier), and compliance auditing.

Role based access involves ensuring only those employees who require access to do their job have access to the minimum amount of information necessary. Access permissions should be documented, remain up-to-date and be managed consistently, preferably by a central authority within the public body. Access to personal information stored electronically should be logged and routinely audited.

Technical controls are rules about what technology requirements must be met to ensure personal information protection. For example, any new technology procured that processes personal information must have role based access, logging and audit capability. All mobile devices that store personal information must be encrypted and remotely wiped in the event of loss. Any linkages of personal information that results in the creation of new personal information must not occur without completion of a PIA.

Physical controls are rules about what physical security is required to properly secure personal information. For example, servers containing personal information must be stored in a locked room with limited access. Personal information must not be left unattended, including in locked cars, when removed from the office for business purposes.

[9] ATIPP Act, RSY 2002, c.1, section 33.

vii. Privacy breach management

The policy will need to address how the public body will manage a privacy breach. Knowing what to do in the event of a breach is essential to mitigating the risks associated with a breach and preventing recurrence.

The policy should specify who is responsible for managing a breach, such as the privacy officer; if containment must occur; when to report to executive and when to involve others as appropriate, such as ICT, legal services, and communications; the process of determining whether to notify the individuals affected by the breach and what criteria will be used to determine whether notification of individuals is required, and the form of notification that will occur (recognizing direct notification is the best); when to involve other parties, such as police and the IPC; and the process of investigating the cause of the breach and managing prevention.

viii. *Complaints management*

The policy will need to address how individuals can challenge a public body's compliance with the ATIPP Act.

As previously mentioned, to obtain access to or correct a record, the ATIPP Act has a process whereby the public can make those requests through the Records Manager. There is no such process in the ATIPP Act for management of complaints about a public body's privacy management. As such, public bodies should establish a complaints management process to manage these complaints. Having a complaints management program demonstrates accountability for compliance with the ATIPP Act. It will also enable the public body to evaluate, through the process of resolving complaints, the effectiveness of its privacy management program. If complaints cannot be successfully resolved through the public body's complaints management process, the complainant can be informed that he/she can make a complaint to the IPC who has authority to investigate complaints about compliance with the privacy requirements of the ATIPP Act.

c) Risk assessment tools

Privacy risks evolve over time and the only way to effectively assess and manage privacy risks is to conduct a privacy impact assessment (PIA). Use of a PIA is an essential component of a privacy management program as it allows the program to continually identify any new risks associated with the collection, use or disclosure of personal information and ensure the information is properly managed in compliance with the ATIPP Act.

At minimum, a public body should complete a PIA for all new projects involving personal information, such as the development of an electronic system that will process personal information and for any new collection, use or disclosure of personal information. PIAs should also be conducted for significant modifications of existing systems, programs or

activities. For example, the following should trigger a requirement to complete a new PIA:

- new types of personal information will be collected,
- changes will be made in the way personal information is used or disclosed,
- personal information previously collected will be contained in or transported through a new information communications technology system,
- personal information will be linked with information from other public bodies or third parties,
- system access is being changed so that new categories or groups of individuals will have access to personal information,
- there are new security risks to the protection of personal information,
- the retention period for personal information will be changed,
- access by individuals to their own personal information will be negatively affected.

To ensure PIAs are conducted, public bodies should include a requirement to complete a PIA in policy and develop procedures for completing PIAs, such as by incorporating PIA requirements into business processes including procurement, contracts management, and ICT development. The privacy officer should be involved in completing PIAs in order to bring the necessary privacy expertise.

The same considerations apply to security threat risk assessments (STRAs), tools that should be used to assist a public body to comply with security requirements under the ATIPP Act. STRAs should either form a part of a PIA or be performed separately but alongside a PIA where appropriate.

d) Training

Having an effective privacy awareness training program is an essential component of a privacy management program as privacy protection will not occur if employees are unaware of their responsibilities associated with privacy protection. Numerous studies have demonstrated that the number one cause of privacy breaches is due to lack of awareness by staff of the rules required to protect privacy.

For a privacy management program to be effective, employees must be trained to know of and follow the policies and procedures put in place by the public body to protect privacy. Once trained, employees should be able to recognize and address privacy protection issues as they arise. This recognition by employees will lead to development of a privacy aware culture. Training should be *mandatory* for all employees and tailored to their specific duties.

There are many ways in which a public body can deliver training. Examples include incorporating training into existing processes such as orientation upon hiring and performance management, developing training modules to be completed by employees on a periodic basis, delivering presentations and workshops, event driven news blasts, and

monthly newsletters.

e) Service provider management

In the ATIPP Act, "employee" is defined to include "a person retained under a contract to perform services for a public body."[10] This means that any service provider is considered, for the purpose of the ATIPP Act, an employee of the public body. Therefore, the public body is responsible to ensure the service provider complies with the ATIPP Act for personal information collected, use and disclosed as part of the provision of services. As such, management of service provider contracts is an essential component of a privacy management program.

Procedures should be developed for ensuring contracts with service providers include:

- limiting collection, use and disclosure of personal information by the service provider to specified contractual purposes;
- taking reasonable security measures to protect the personal information;
- requiring compliance with privacy policies and other applicable privacy protection controls of the public body, including with respect to storage, retention and secure disposal;
- requiring notice to the public body in the event of a privacy breach;
- controlling sub-contracting;
- restricting access to service provider's employees who require access to the personal information to perform the service;
- training the service provider's employees who have access to the personal information;
- requiring the service provider to have its employees enter into agreements agreeing to comply with service provider's privacy obligations under the contract;
- addressing the sale of or change of control in the business, including through insolvency or bankruptcy;
- enabling the review or audit the service provider's compliance at any time with the privacy protection provisions contained in the contract;
- indemnifying the public body from any liability associated with a violation by the service provider of the privacy protection provisions of the contract; and
- returning or destroying personal information upon demand or upon termination for any reason.

In larger public bodies, program procedures should ensure collaboration between the privacy officer and the public body's procurement and contracting staff.

[10] ATIPP Act, RSY 2002, c.1, section 3.

f) Communicating with individuals and demonstrating accountability

A number of the ATIPP Act's requirements involve communication between public bodies and individuals (including the public body's employees) whose personal information they collect, use or disclose. These communications occur through the requirement to give notice of collection; requiring, in some circumstances, consent to indirectly collect personal information or use and disclose it; responding to requests by individuals for access to or correction of their own personal information; or providing notice to an individual when his/her personal information may be provided to a third party who requested access to this information.[11] An essential component of a privacy management program is, therefore, to ensure these communications are conducted in accordance with the ATIPP Act requirements. These communications should include informing individuals of their privacy rights and of the public body's program controls. All communications should be expressed in clear and easy-to-understand language.

[11] ATIPP Act, RSY 2002, c.1, sections 26 and 28.

B. Ongoing Assessment and Revision

This part outlines how a public body can ensure their privacy management program is effective. Like all management tools, privacy management programs need to be kept current. They should remain practical and effective in the face of changing services, technology, administrative structures and applicable legislation. A public body cannot take a snapshot approach by creating a privacy management program that does not evolve with legal requirements and business needs.

To ensure a public body remains accountable in meeting its ATIPP Act obligations, it must assess and revise its privacy management program regularly and consistently. This part outlines the ways in which a privacy management program may be maintained in order to meet these objectives.

3) Develop an Oversight and Review Plan

The privacy officer should develop a plan to review and revise the program on a regular basis. The plan should include when and how the review will occur and what it will entail. Operational changes that impact the effectiveness of the program should be considered as part of the review along with the adequacy of program resources, reporting, communication, and integration into the public body's business processes.

4) Assess and Revise Program Controls

It should be a requirement in the review plan that program controls are assessed on an ongoing basis in order to evaluate whether revision is necessary to mitigate the risks to privacy protection. Revision may be necessary to address:

- new privacy or security threats and risks from within or external to the public body;
- risks to privacy identified in complaints and breach management, audit findings, PIAs, and STRAs;
- changes in privacy laws and decisions of the IPC;
- changes in the public body's mandate, authorities, duties or functions, statutory or policy framework, organizational or management structures, budget resources, or operating programs or activities;
- inadequate employee privacy awareness;
- poorly managed service provider relationships;
- improper use of privacy risk management tools, and
- ineffective communications.

Periodic or random audits should be used as part of assessing the program controls, particularly where the risks to privacy protection are considered high. Audit processes should include employee interviews and file reviews, both of which should evaluate compliance with objective criteria. External audits may be warranted in some cases, notably where a larger public body has suffered a significant privacy breach. In such cases, consideration should be given to retaining a qualified third party to perform the audit or review. Regardless of whether they are routine or triggered by a breach, internal and third-party audit reports may help establish due diligence in response to an investigation or review by the OIPC.

Revision of the program controls should be slated in the review plan for annual review or sooner if required to mitigate any significant risks to privacy identified through assessment of the program controls. The review plan should include a requirement that the public body's personal information inventory is updated annually to ensure any new collections, uses and disclosures of personal information are included.

Communications about changes to the program controls should be communicated to employees promptly in order to mitigate risks.

Conclusion

Public bodies need to be vigilant in the area of privacy protection because public trust and confidence are at stake. Privacy management programs must be documented and transparent. In the event of a complaint about non-compliance with the ATIPP Act, a privacy breach, or about privacy management, public bodies will want to be able to demonstrate its ability to properly manage risks to privacy. Being able to do so will help to allay the concerns of Yukoners and enable the public body to respond to questions from the OIPC about the public body's accountability for compliance.

There is not a one-size-fit all privacy management program. The building blocks are scalable and should be tailored to the size and mandate of the public body and the amount and nature of the personal information it has in its custody and control.

It is hoped that the guidance in this document will assist public bodies in Yukon to effectively protect privacy in accordance with the ATIPP Act and be able to demonstrate accountability for privacy protection.

Privacy Management Program – At A Glance

Building Blocks – Privacy Management Program Essentials

Public body commitment	**Executive management support**	• Executive management of the public body has: o committed to providing the resources necessary to develop, implement, assess and revise the privacy management program, o designated and empowered a privacy officer at the appropriate level in the public body to be responsible for managing the privacy management program and to monitor compliance with the ATIPP Act, and o clearly defined in policy the role and duties of the privacy officer.
	Privacy officer	• The role of the privacy officer (or privacy designate) is defined and is fundamental to business decision-making processes. • The role is responsible: o for the development and implementation of the program controls, o to ensure privacy protection is built into every major function involving the collection, use or disclosure of personal information, and o to assess and revise the program as necessary to ensure compliance. • The responsibilities of the role to monitor compliance with the ATIPP Act are communicated throughout the public body. • Adequate resources have been identified to support the role and put into place.
	Reporting	• Reporting mechanisms are established and reflected in the public body's program controls.

Program controls	**Personal information inventory**	• The public body is able to identify: o the personal information in its custody or control (amount, categories, number of individuals whose personal information it holds, and location), o authority for the collection, use and dis-closure of the personal information, and o the sensitivity of the personal information
	Privacy policies and procedures	• Privacy policies and procedures exist that ad-dress: o purpose and authority for collecting, using and disclosing personal information, o indirect collection of personal information, o requirements for consent and notification, o how to ensure the personal information is accurate and kept up to date, o individual access to and correction of personal information, o retention and destruction or disposal of personal information, o how to secure the personal information including administrative, physical and technological controls, o how a breach of privacy will be managed, and o a process for responding to privacy- related complaints.
	Risk management tools	• Risk assessment tools, such as PIAs and STRAs are used where appropriate and the requirement to use these tools are included in policy.
	Training	• Employees participate in mandatory privacy awareness training and receive additional training as is necessary to ensure awareness of the policies and procedures.
	Service provider management	• Procedures exist and are applied to manage personal information involved in service provider contracts.
	External communications	• Communication with individuals meet the re-quirements of the ATIPP Act, individuals are in-formed about their rights under the ATIPP Act and about the public body's complaints manage-ment process, and individuals are informed they can make a complaint to the IPC.

Building Blocks – Ongoing Assessment and Revision

Oversight and review plan developed	• A plan to review and revise the privacy management program exists and includes: o a requirement that the program controls are assessed on an ongoing basis to mitigate risks to privacy protection, o a requirement to conduct periodic or random audits on the effectiveness of the program controls, o revision of the program controls on an annual basis or sooner if necessary to mitigate the risks to privacy, and o communication with employees about changes to the program controls.
Program controls are assessed and revised	• The review is carried out in accordance with the plan and the program controls revised as necessary and communication with employees occurred.

Appendix A

This appendix identifies resources that may assist public bodies in designing, implementing and maintaining their public body privacy management program.

ACA – ATIPP Compliance Assessment
Contents of a Response
Duty to Assist
Privacy Breach Response and Privacy Breach Checklist
Video Surveillance Guidelines
Privacy in an Emergency in Yukon
10 Workplace Tips for Protecting Personal Information on Mobile Devices

These resources are located on the OIPC's website at:
http://www.ombudsman.yk.ca/ipc/useful_tools/

Security Self-Assessment Tool: This tool will help you assess your organization's security measures and offers guidance on minimum security requirements in 17 different categories. It was produced jointly by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the OIPC BC.

This resource is located on the Privacy Commissioner of Canada's website at:
https://www.priv.gc.ca/resource/tool-outil/security-securite/english/AssessRisks.asp?x=1