ᑲᑎᒪᔨ ᓄᓇᕗᑦ ᐱᖃᓐᓇᕐᓂᖅᓴᖅ
Building Nunavut Together
Nunavuliuqatigiingniq
Bâtir le Nunavut ensemble

AM

# Government of Nunavut

# Privacy Management Manual

# Introduction to the Privacy Management Manual

The Privacy Management Manual (PMM) is a comprehensive set of tools and resources to be used by all employees of the Government of Nunavut to successfully implement the privacy provisions of the *Access to Information and Protection of Privacy (ATIPP) Act.*

All employees are required to familiarize themselves with the PMM as the *ATIPP Act* holds each employee accountable for the privacy of personal information under the custody and control of the government.

The PMM includes the following sections:

1. Privacy within the Government of Nunavut
   This section explains the privacy concept, highlights the main requirements of the *ATIPP Act* as they relate to the collection, creation and handling of personal information, and provides advice and tips for the privacy compliant administration of all GN programs and activities.

2. Privacy and Communications
   This section provides guidance to communications staff members and other employees with communications issues, when dealing with personal privacy in their role.

3. Creating Records in the Context of ATIPP
   This section provides all employees with guidance on how to appropriately create records that will be used by the Government of Nunavut. This section provides tips on what can be done to ensure the records we create are privacy compliant.

4. Privacy and Contracting
   This section is relevant for all employees who contract work for the Government of Nunavut. It ensures employees are aware of privacy and access issues that can arise when creating contracts with outside contractors. This section provides tips on what should be included in contracts.

5. Privacy and Human Resources
   This section is specifically relevant to those working in human resources related fields, including those in supervisory roles.

6. Comprehensive Procedure for the Handling of Privacy Breaches and Incidents
   This comprehensive procedure for the handling of privacy breaches and incidents supports the GN's Privacy Breach Policy by providing detailed procedures to assist the ATIPP Manager and ATIPP Coordinators when dealing with public bodies subject to the *ATIPP Act*, in preventing, responding to, and investigating privacy breaches and privacy incidents. It is complemented by forms to be used when reporting and investigating privacy breaches.

7. Comprehensive Procedure for the Handling of Privacy Impact Assessments
   The Privacy Impact Assessment (PIA) process is a risk management instrument that supports compliance with the requirements of the *ATIPP Act* as they relate to privacy protection and with generally acceptable principles. It provides an approach to assess the privacy implications of all initiatives of public bodies that are subject to the *ATIPP Act*.

This section supports the Privacy Breach and Incident Policy by providing a detailed procedure for the conduct of Privacy Impact Assessments (PIA). It is accompanied by forms and other tools that aim to facilitate the conduct of PIAs.

8. Procedure for the Conduct of Privacy Inspections and Privacy Compliance Audits

This document is designed to assist the ATIPP Manager and ATIPP Coordinators in their efforts to prevent privacy incidents and privacy breaches by identifying existing gaps and weaknesses in the systems, policies and practices of public bodies.

## Table of Contents

# Section 1:
# Privacy Protection within the GN

## Contents

# 1. Introduction

As a result of their daily interactions with the residents of Nunavut, GN employees often become an intricate part of the lives of these individuals. Consequently, they end up collecting vast amounts of personal information about these residents, some of which is very sensitive. Because the collection and the creation of personal information comes with enormous responsibilities, it is essential that these employees (as well as their superiors) act in the most professional way and treat the personal information under their custody and control with the highest degree of respect and in keeping with the legal and policy requirements that govern the programs that they administer.

This document explains the privacy concept, highlights the main requirements of the *ATIPP Act* as they relate to the collection, creation and handling of personal information, and provides advice and tips for the privacy compliant administration of all GN programs and activities.

# 2. What Privacy is Really About

Most people assume that privacy is about protecting the confidentiality of the personal information under our control. This assumption is not entirely wrong, but it presents a largely incomplete picture of what privacy is really about. For instance, the main component of privacy protection is not confidentiality but instead the limitations that we impose upon ourselves in relation to the amount of personal information that we collect. The smaller the amount of personal information we collect, the lower the need to implement security measures to protect its confidentiality. Collecting less personal information also means lower risks of improper use and modification and lower costs on storage, maintenance and updating.

As a government, we cannot operate our various programs and fulfill our responsibilities without collecting certain types of personal information in order to determine benefit eligibility of our clients, enforce the various laws for which we are responsible, administer correction programs, provide health-care services, educate our youth and protect the environment.

The key objective in all the above listed circumstances is to reach a balance between the need to fulfill our legal obligations and other requirements, and demonstrate a profound respect for the privacy rights of all individuals – clients, employees and other community members. Limiting the collection of personal information to what is absolutely necessary makes sense.

Our privacy obligations are also determined in large part by each individual's expectations. There is no scientific way to determine whether an individual would consider a particular action on our part as an undue invasion of his or her personal privacy. Our decisions to collect or create personal information and how we handle it must also be guided by the values and principles of honesty, integrity, fairness, justice, respect, civility, decency and dignity. Ultimately, the way in which we protect the privacy of the individuals with whom we interact determines in large part the level of trust that the public is prepared to place in the GN as a whole and in each of the public bodies that make up our government.

# 3. Operational and Administrative Context of Privacy, Confidentiality and Security

### The Privacy, Security and Confidentiality Concepts

Although the privacy, security and confidentiality concepts operate in unison to guarantee the adequate protection of individuals' personal information, they refer to three different things:

- Privacy is the determination of what is allowed to be done with individuals' personal information;
- Security refers to the measures that we implement to prevent inappropriate use or handling of personal information;
- Confidentiality, a subset of security, refers to the restrictions that limit access to that personal information.

The security and confidentiality concepts are explained below to allow us a better understanding of what they entail and how they contribute to enhancing the protection of everyone's privacy.

### Security

In the broadest sense, security aims to protect all categories of sensitive information (personal and non-personal) and valuable assets from threats and risks. Additionally, it protects employees from threats and acts of intimidation, blackmail and violence. Within the narrower privacy context, security means the use of policies, procedures, physical design, physical and electronic devices as well as personnel-related safeguards (background checks and awareness) to protect the personal information under our control. Security measures provide protection from a wide range of threats that could bring liability for the GN, cause harm to an individual or even a loss of life, produce unfair decisions, cause embarrassment or undue media attention, and more. Threats or risks include:

- Unauthorized access – loss of confidentiality;
- Unauthorized use;
- Unauthorized modification – loss of integrity;
- Unauthorized destruction – loss of availability of the information for proper and legitimate decision-making.

The implementation of adequate and well-designed security measures also brings other benefits by contributing to:

- Minimizing or reducing:
    - The risks of interruptions affecting departments' operations and the delivery of services to the public;
    - The costs associated with the protection of sensitive information – including the protection of the equipment and facilities that we use to process and store that information;
    - The waste in resources that may result from over-protecting information or assets or from protecting information or assets that do not require protection;
    - Administrative and operational inconveniences.

- Maximizing or increasing:
    - Access to the information that is required by the employees who need it to perform their duties;
    - Efficiency and effectiveness in the delivery of the services provided by public bodies;
    - Reporting and accountability;
    - Transparency and the effective exchange of essential information with the public.

Because officers and employees are the ones who make the decisions to collect, create, use, share, retain and protect the personal information under the control of their respective bodies, they are the first line of defense against threats and risks. Employees have the greatest impact on the successful protection of personal information under the control of the GN.

## Confidentiality

Confidentiality means restricting access to information of a sensitive nature to the smallest number of individuals possible. Access must be granted on a clear need-to-know basis, following these three premises:

- Only those who have a demonstrable requirement for information and who have been duly authorized should have the **privilege** of accessing it – **not a right** to access it;
- These individuals must be worthy of the trust that we put in them, and they must clearly understand their roles and responsibility in protecting it; and
- Access by those individuals must only be granted at the time when they really require access to the information, and only for the amount of time during which they require access for the performance of their legitimate duties – e.g. they must not deliberately retain the information or their ability to access it longer than is necessary.

It flows from the following three premises that the rank, title and role of an employee, manager or elected official are not necessarily relevant when it comes to determining whether that person should have access or not to sensitive information. The only criterion is the clear requirement for performing that person's immediate duties. In this context, the notion of "duties" refers to:

- The making of a business or professional decision; or
- The performance of a business-related or professional activity.

Strictly speaking, administrative convenience and cost-saving factors do not by themselves justify access to personal and other sensitive information, especially when such access is likely to cause an intrusion into the privacy of an individual. Other more compelling reasons must always be part of the decision to create, collect or share sensitive personal (and sensitive non-personal) information. Similarly, other circumstances that fit under the "nice to know" considerations definitely do not meet the need-to-know threshold. The key is to assess the benefits and the risks associated with each activity, project, program or system for which the personal or other sensitive information is to be used.

The sensitivity of personal information is normally determined by the gravity of the consequences that could result from it being compromised (unauthorized access, use, modification or destruction).

The process we use to assess those consequences is known as a Privacy Impact Assessment (PIA). This process is described in detail in the GN manual for PIAs.

## 4. What Privacy Means to Each Individual

One common assumption we must avoid is that we should treat other people's personal information like we would want them to treat our own personal information. First, this approach is based on the assumption that what is acceptable to us is acceptable to others, regardless of their personal preferences. Second, it fails to account for cultural and other differences as they relate to what people consider respectful, decent and compatible with their sense of dignity. From a privacy perspective, assuming that another person "will not mind" is one of the worst mistakes that one can make. Instead, it is our duty to handle the personal information of other individuals – i.e., clients and employees alike – in the way that **they** consider acceptable, and most of the time this can only be determined by asking them what they think.

## 5. Privacy Protection and the *ATIPP Act*

Part 2 of the *ATIPP Act* governs the creation, collection, use, disclosure/sharing, accuracy, protection, retention and disposition of personal information by public bodies. It also grants individuals the right to request the correction of their own personal information. Part 1 grants those individuals a right to request access to their personal information.

The rights accorded by the *ATIPP Act* are based on the following definition of "personal information", a term defined as "*information about an identifiable individual*". This includes all factual and subjective information that may exist about an individual, as well as any views and opinions that have been expressed by other individuals about that individual. Only identifiable "individuals" are eligible to privacy rights under the *ATIPP Act*. Corporations and non-profit organizations cannot claim to have any such rights under the Act. The GN may still have confidentiality obligations, either required by other acts or regulations, or by contract.

Generally speaking, Part 2 of the *ATIPP Act* establishes rules that limit the collection and creation of personal information to only that which we absolutely need to fulfill our legislated obligations and perform our legitimate activities. It also states personal information must only be collected when it is required (not in anticipation of a future need), and that it must normally be collected directly from the individual to whom it pertains, except in those rare circumstances where direct collection could defeat the purposes of the collection (e.g., investigation) or result in the collection of inaccurate information (e.g., reference checks conducted as part of the staffing process).

The individual from whom we collect that personal information must be fully informed of all the implications of the collection, and once it has been collected or created, the personal information must only be used and disclosed as permitted by the individual to whom it pertains or in accordance with the *ATIPP Act*.

Once personal information has been involved in a decision-making process that directly affects an individual, it must be kept for a minimum period of one year after the last time that it was used in

the decision-making process. The Act also requires that public bodies implement reasonable security measures to protect the personal information under their control from unauthorized access (confidentiality), modification (integrity), use and destruction.

Finally, the *ATIPP Act* establishes a complaint mechanism whereby individuals can ask the Information and Privacy Commissioner of Nunavut to investigate any complaint that they may have regarding alleged non-compliance by a public body with any of its provisions.

## 6. For More Information on the Subject of Privacy Protection

The other documents that comprise this series provide explanations and advice on the best ways to ensure the adequate protection of the personal information that is used by GN public bodies. Private sector organizations must follow the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and must take reasonable measures to protect the personal information they collect, use and disclose. More information on PIPEDA can be found by contacting the Privacy Commissioner of Canada.

# Section 2:
# Privacy and Communications

## Contents

# 1. Dealing with Personal Privacy as Communications Staff Members

Communications Officers are frequently exposed to situations or circumstances that involve personal information which has entered the public domain. In many instances, it is the individual to whom the personal information pertains who has alerted the public about his or her personal situation, whereas in other cases the individual is a victim of an unwanted disclosure. Whatever the situation, Communications staff members always have to use caution when they present the government's position in regards to a particular situation since what they say and how they say it may result in a breach of Part 1 of the *Access to Information and Protection of Privacy (ATIPP) Act* or add to the unfortunate circumstances that affect the individual(s) involved.

# 2. Publicly Available Personal Information

First and foremost, it is important to address one of the most enduring myths according to which personal information that is publicly available is not protected by the *ATIPP Act*. While it is true that paragraph 48 (t) of the Act states that personal information may be disclosed "*where the information is otherwise available to the public*", this provision only refers to situations where the personal information is publicly available **in the same context** as the one in which it appears in a government file, such as in the telephone book. To use the same telephone book example, the only information that can be obtained or inferred are the following facts:

- The individual's likely language background, cultural origin and gender – which can be inferred from the individual's name;
- Depending on the circumstances, the individual's approximate age – based on the "trend of the day" in parents assigning first names to their children;
- The individual's socio-economic background and lifestyle – which can be assumed from the individual's home address.

Finding this information in the phone book does not signify any interactions or transactions with a public body. Alternatively, if this same information were revealed by a public body, the likelihood of interaction or transaction with that public body would exist, (or at least the interest that the public body has in that individual). This is why the disclosure, by a government public body, of even the most insignificant element of personal information that may already be publicly available would, under most circumstances, be considered a breach of section 48 of the *ATIPP Act*.

To avoid such a breach follow this rule: when in doubt, refuse to confirm or deny the existence of any personal information about an individual. For example: If a reporter calls to confirm the medical state of a patient at the hospital, by stating that you can't give out their medical condition, you have confirmed that they are actually in the hospital. The appropriate response would be, "I'm sorry, I can't confirm nor deny whether or not that person is a patient at our hospital as it is prohibited by the *ATIPP Act*".

## 3. Handling Media Inquiries

Generally, media inquiries about an individual's particular situation must be responded to in a neutral manner without revealing the fact that the public body may or may not have had any interaction with the individual. Where the situation revolves around the application of policies or procedures pertaining to the individual's personal situation, Communications staff members must limit their explanations to the relevant requirements of the policy or procedure and leave things at a generic level. When asked specifically about one identifiable individual's personal situation, the answer should always be that, "discussion about any specific individual is prohibited by the *ATIPP Act*".

The fact that the individual has offered details about his or her personal situation to the media can in no way be interpreted as implicit consent by the individual for the public body to confirm the information or respond to the allegations in a direct way. Consequently, Communications staff members must never disclose any facts or make any comments that may confirm the individual's identity as a client (or other status) of the public body or reveal the existence of any kinds of interaction with the individual. Misleading or false information disclosed by an individual shall be addressed in the most neutral manner possible or simply by a statement such as "due to privacy considerations, we cannot comment on any issue that may pertain to an identifiable individual". However, the individual can give their express written consent to have the GN release information.

As a general rule, the GN does not comment on matters that are before courts, tribunals, public inquiries, and other legal proceedings, other than to confirm that the GN is taking legal action, or is defending itself against legal action. The GN cannot give appearance that it is trying to influence the court or tribunal. There may also be publication bans and sealing orders to consider. It is recommended that Communications staff members contact legal counsel for advice before commenting on legal matters. GN departments should contact the Legal and Constitutional Law Division of the Department of Justice.

## 4. Lists of Professional Contacts and Mailing Lists

The creation of a list of professional contacts by Communications staff members is perfectly legitimate provided that it is only made available to those individuals who have an absolute need to know and that it is used only for the purpose of contacting the individuals within the context that has been agreed upon at the time when the Communications staff member received the business card or the information from the individuals. A contact list must never be used for mass mailings or shared with other parties, including within the public body. It must also be protected from unauthorized access and modification.

The creation of mailing lists is also a legitimate undertaking as long as all of the individuals whose names are included in the lists have provided fully informed consent – i.e., they have been told exactly what the mailing list is going to be used for and that they can have their names removed from it at any time. The creation of mailing lists must be the subject of a privacy impact assessment (PIA) to ensure that they are administered in accordance with the *ATIPP Act* and the generally accepted privacy principles. Details about the PIA process can be obtained by consulting the GN's

PIA policy or by contacting the ATIPP office within the Department of Executive and Intergovernmental Affairs.

## 5. Surveys and Client Satisfaction Research

Surveys and client satisfaction research activities must be done in total conformity with the *ATIPP Act* and the generally accepted privacy principles. Consequently, a privacy impact assessment (PIA) must be conducted before any contract is signed with a private firm that is hired to manage the process (see the brochure titled Privacy and Contracting for more details about the contracting process) and before the commencement of any such activity.

As much as possible, surveys must be done in a manner that does not generate the collection or creation of identifiable information about individuals, and the individuals must be told about their rights under the *ATIPP Act* before they are asked to answer questions. Surveys and client satisfaction research activities that are conducted over the Internet must be designed in such a way as to minimize the risk that identifiable information be collected or generated by the computer systems – IP addresses, etc.

# Section 3:
# Creating Records in the Context of ATIPP

## Contents

# 1. Importance of a Sound Approach to the Creation of Information and Records

Creating records is such a routine activity that most of us never give it much thought. We create records because our intuition tells us that certain facts, decisions and actions should be documented, by reflex from old habits or simply because we have been told to do so. Sometimes we choose to not document certain facts, decisions or actions because we don't see the necessity or because we fear the repercussions that may result from other individuals eventually gaining access to that information. In order to ensure that all necessary records are created, and that only needed information is retained, employees require clear direction and operation guidelines. Following the guidelines contained in this document will help you avoid creating:

- records that are created without proper authority;
- records that may not contain the information that they should contain;
- records that contain inaccurate information;
- records that may not exist in the right format, thus preventing them from being used for the purposes that they are supposed to serve;
- records that may not present the information in a useful manner; or worst of all,
- records that may contain statements that later become a source of embarrassment for their author or for the public body.

# 2. Creating Records in the GN

## Administrative Records

The information that is required to ensure the cost-effective internal management processes of public bodies, such as finance, records management and human resources are, for the most part, defined by legislative and policy requirements as well as by generally accepted practices within each of those disciplines. But even so, questions will always emerge around the issue of "what exactly are we supposed to document and how?"

## Operational Records

Since the categories of information that support operational requirements are specific to each public body and each program, there are no universal standards to go by. Each public body faces the challenge of having to develop its own standards and procedures for their creation, collection and handling, based on the functions and activities that they are intended to support and the relevant legal requirements, whenever they exist.

In most cases, the records that we create about our clients contain information received from the client himself or herself, but sometimes the information may come from another government institution, a private sector organization (e.g., past or present employer) or a member of the individual's family (e.g., in the case of students and elderly). In many instances, the challenge is to decide whether or not to accept or document the information that is being offered.

## Why We Create Records

Essentially, we create records to capture the important elements of information that will later:

- lead to and support the decision making processes at all departmental levels;
- serve to enforce accountability in regard to the important decisions that we make and the actions that we take;
- provide a historical perspective of important events, decisions and actions so that these actions and decisions can be better understood, that lessons can be learned and that mistakes can be avoided in the future;
- provide evidence that can be used to respond to, or initiate administrative and legal challenges;
- allow us to report our activities to the Legislature, the Financial Management Board or another authority;
- provide reliable data and statistical figures that can be analyzed for policy development and program assessment and evaluation;
- support all our administrative and operational processes, such as those by which we:
    - communicate with our clientele – individuals and businesses;
    - try to understand and respond to our clients' individual needs and expectations;
    - develop our knowledge and expertise;
    - develop and maintain a fruitful relationship with other institutions that support our objectives;
    - respond to the expectations of the residents of Nunavut as they relate to accountability and transparency;
    - ensure the cost-effective delivery of services to our clientele; and
    - fulfill our legislative obligations.

The information that is collected and created while fulfilling our responsibilities must be documented and stored in a way that facilitates its retrieval for future operational and legal requirements, including responding to requests received under the *ATIPP Act.* Furthermore, it must be adequately safeguarded to protect its confidentiality, integrity, availability and value.

# 3. How to Create Meaningful and Privacy Compliant Records

## Have a Clear Objective in Mind

The best way to create a meaningful record is to have a clear objective in mind in terms of what we want a document to accomplish over the coming weeks, months and years. If you cannot think of a specific objective for it, it may be that there is just no need to create it. Once the decision has been made to document certain facts or views, the clearer the objective the easier it will be to decide what to include and what not to include in the document.

## Include the Right Information

Within the GN the records that we create generally aim to convey a legal, policy, technical or business message, and are often intended to support the delivery of services to our clientele. These purposes must be reflected in the contents, format and style of each document. Personal opinions should be left out unless they take the form of properly formulated options, suggestions or recommendations that are intended to support the decision-making process (there is more on the expression of personal opinions in a later section of this brochure).

An important point to remember is that the larger the audience the less control we will have over the confidentiality aspect of the information that it contains. Therefore, documents that are intended for a large audience should not, as a general rule, contain sensitive information.

## One Document per Subject; One Subject per Document

The inclusion of information about multiple subjects in the same document poses numerous problems:

- it makes it impossible to find a title that reflects all the subject matters discussed in the document, thus complicating the record classification process and the retrieval of the information;
- it makes it virtually impossible to enforce the need-to-know principle, because a person who looks at the information that they need to access within the document is at the same time exposed to the information that pertains to the other subject matters that are also discussed in it, even if they don't need to see that other information;
- if a request under the *ATIPP Act* is received for information that is discussed in a particular document, the whole document will have to be reviewed and possibly disclosed to the applicant, **including all of the information contained in it that is not relevant to the access request**, unless these portions contain material that qualifies for an exception to the right of access.

Consequently, the rule is that **whenever possible**, we should limit the discussion to one subject matter per document as this is the most cost-effective way to work, classify, organize, retrieve and protect the GN information. The above considerations also suggest that the use of bound notebooks is not a good idea, even if these notebooks could technically in some cases qualify as "transitory documents" (there is more on the subject of transitory documents later).

## Writing Style

As previously mentioned; the records that we create generally aim to convey a legal, policy, technical, or business message. They are often intended to directly support the delivery of services to our clientele. Consequently, they do not have to be fancy or enhanced by beautiful turns of phrases. They must be short, to the point and clear. The use of a direct style is preferable in most cases. Each word that we include in a text adds to the wide range of interpretations that can be given to it, something that may later cause problems. Whenever possible, point forms, graphics and tables should be used instead of long and winding narrative explanations.

The style (technical, formal, casual, etc.) must normally reflect the purpose of the document and the audience for whom it is produced. The general rule is the broader the audience the more accessible the language must be. Plain language also facilitates translation into the other official languages.

When writing reports and other internal documents that are likely to affect the rights, obligations, benefits or privileges of our clients or employees, it is advisable to use the third person approach – e.g., "the auditor", "the undersigned", etc. – instead of using the pronoun "I". This approach, albeit more formal, detaches us from the positions that we express, and often reduces accusations of biases and allegations of potential conflicts of interests. Psychologically, it also brings us to feel more detached and objective during our analysis, something of crucial importance if the record is later the subject of an access request under the *ATIPP Act* or a subpoena issued by the Court.

In correspondence, it is important to remember that you are writing on behalf of the GN; not on your own behalf, and this should be reflected in the style and tone of the letter.

## Document Title

At some point during the record creation process, we must decide on the title that reflects the content or the objective of the document. This may happen at the very beginning of the record creation process or, at times, it will come at the very end, once we have a clear idea of its content. Ease of retrieval by us and by others should be the main key criteria when assigning a title to a new document. Since we only have 30 calendar days to respond to an ATIPP request, the longer it takes for those who conduct the search for the requested records to figure out what titles to look for the more difficult it will be for the public body to meet the legislated deadline for responding to requests.

## Document Structure

A logical structure is one that allows the reader to follow the path taken by the author of the document when analyzing, asking questions or reaching a conclusion on an issue or a subject. It is also one that makes it easier for ATIPP coordinators to determine what to disclose and what to protect in the event of an ATIPP request. It is worth noting that the title of a document does not automatically determine whether or not it is protected under the *ATIPP Act* – the substance of that document is what is considered in relation to disclosure. For example, a briefing note is not automatically protected under Section 14(1) unless the substance of the record is advice or recommendations.

Each document has its own objectives which dictate a specific approach in terms of structure and style. The following structure is generally suitable for most documents identified as reports, briefing notes, memos, notes to file, and other documents that present facts, analysis, conclusions, options and recommendations:

- **Introduction**

  This section is used to briefly explain the purpose of the document;

- **Body**

  The body of the document is used to present:

  - a description of the relevant facts pertaining to the subject matter and the general context surrounding those facts;
  - where applicable, the chronology of events;
  - where applicable, a description of the various conflicting versions, arguments and interests at stake;
  - where applicable, the technical, political, organizational and other relevant considerations.

  Important note: the body of the document must not be used to present hypothesis or assumptions or the result of the analysis as this could compromise the objectivity and the integrity of the factual description of the circumstances or situation.

- **Analysis and Conclusions**

  Where applicable, this section is used to describe the methodology that was used for the analysis as well as the considerations that served as a basis for the conclusions.

- **Options**

  This section is used to present the various courses of action that are available to the decision-maker(s).

- **Suggestions and Recommendations**

  Where applicable, the suggestions and/or recommendations are presented under this heading.

- **Annexes**

  The annexes are usually stand-alone documents appended to the main one (and written by different authors) that are meant to supplement (often to add credibility) the main document.

- **Appendices**

  The appendices are used to append copies of the mandate of the author of the document (terms of reference) and copies of the forms that were used to collect information, and document the facts, such as interview notes, minutes of meetings, exchanges of correspondence, and so on, as well as documents that support the facts, the assumptions and the conclusions that are presented in the main part of the document.

# 4. Words, Expressions and Statements to Avoid

## Avoid the So-called "Absolute Words"

Terms and statements that suggest a lack of nuance are likely to be interpreted in an unfavourable way by the media and the public and they often convey generalizations and stereotypes. Examples of such terms include "always", "never", "everyday", "constantly" and "all the time". In addition, terms and expressions:

- are rarely scientifically or statistically demonstrable;
- can even in some contexts be taken as criticism or, worse, as discrimination; and
- may also leave the public bodies vulnerable to attacks during litigation, as the other party would only need to demonstrate that the generalization was excessive to successfully discredit our entire position before the court.

Another good point to remember is to avoid the use of terms and expressions about people and organizations that suggest a permanent character trait: "he is like that...", "she is a...", "this is typical of that employee/client/organization..." and so on. These terms and expressions are profoundly judgmental and disrespectful and they suggest that these individuals or organizations have always acted, and will always act as described in the text.

## The Use of Adjectives and other Qualifiers

When describing facts or situations, it is preferable to avoid adjectives and expressions that may make us sound or appear to be judgmental. Even though adjectives and qualifiers such as "large", "positive results", "encouraging" and "inappropriate" may be acceptable in some situations (such as when they are used to legitimately express a personal appreciation of something), they cannot be supported by scientific or credible evidence and they will, in most contexts, leave us vulnerable to accusations that our perception is biased or that we are prejudiced. The use of descriptive qualifiers that can be demonstrated by physical observation or supported by documentary evidence is much more preferable.

# Section 4:
# Privacy and Contracting

## Contents

# 1. Introduction

Contractors play a significant role in the ability of public bodies to achieve their objectives, and they often have a considerable impact on the decisions that affect the rights, benefits and privileges of the clients of those public bodies and other citizens. Yet, unlike public servants and elected officials, contractors are not generally in direct contact with the members of the public, which means that their actions and decisions are not scrutinized in the same manner as those of employees and elected officials. By extending its provisions to contractors, the *ATIPP Act* imposes upon contractors a certain degree of public accountability, if not by requiring that they openly explain their actions and decisions, by at least subjecting all the information and documents that they create, collect, use and share to the public's right of access and by extending its privacy provisions to them.

# 2. The Status of Contractors under the ATIPP Act

The term "**contractor**" generally refers to all individuals who:

- perform or participate in the performance of services for a public body; or
- deliver or participate in the delivery of services on behalf of a public body,

in a capacity other than as a GN "employee", as defined by the *Public Service Act* (Nunavut). This implies that their reporting relationship is not the same as that which applies to "employees" and that the accountability mechanisms to which they are subject are different than those that apply to "employees".

Section 2 of the *ATIPP Act* defines the term "employee" by stating that "*in relation to a public body, includes a person retained under contract to perform services for the public body*". Consequently, the provisions of the *ATIPP Act* apply to contractors to the same extent and exactly in the same manner as they apply to employees, irrespective of the fact they may:

- be paid or not for their services;
- perform the services on a public body's premises or at another location;
- use or not the equipment provided by a public body to perform the services;
- act as independent contractors (i.e., they signed the contract themselves) or as employees of another person, a private sector corporation or a non-profit organization.

The *ATIPP Act* only applies to those employees of a private sector company who are actually assigned to work on a contract with the GN under which the company may be working – and not to its entire workforce. There can be situations where an employee who benefits indirectly from the contract may be subject to the *ATIPP Act*, but the circumstances of those cases must normally be examined by the ATIPP coordinator for the public body in order to determine their status under the Act. Private sector organizations operating in Nunavut must comply with the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA), and some of the GN's service providers may have legal obligations under provincial health information legislation. Where one legal regime interacts with another it should be clearly identified in a service contract. GN departments should seek legal advice prior to entering into service contracts involving the collection, use and disclosure of personal information.

## 3. The Status of Records Produced by Contractors under the ATIPP Act

Generally, the rules that apply to employees also apply with some minor variations to contractors, which means that, for example, the documents collected or created by a contractor during the course of the performance of a contract for a public body will normally be considered the property of the public body, even if the contractor has kept the original documents or copies of them after the completion of the contract. But there are instances where the contractor's records will likely fall outside the *ATIPP Act*, such as the contractor's patented or copyrighted methodology that existed prior to the signature of the contract and the development of which was not paid by the GN. Contracts must contain provisions that address what happens to the information when the contract is finished; for example a contract could state that once the GN receives the final report, the information will either be returned to the GN or securely destroyed. Public bodies should seek legal advice for every contract or agreement involving the collection, use or disclosure of personal information.

## 4. Copyrights and Patent Rights of Contractors

As a general rule, records collected or created by a contractor, including policy material and other documents prepared specifically for a public body, are the sole and exclusive property of the GN. Consequently, contractors are not allowed to include any statement by which they claim any shared or exclusive copyright, patent or any other right in regards to those documents. Documents that contain such claims shall be refused by public bodies, and the contractor shall be asked to remove the improper statements from all versions and copies.

To reduce the possibility of any such conflicting or confusing situation, it is preferable that public bodies clearly assert their exclusive authority over all records and information collected, obtained, produced, or otherwise acquired by contractors during the course of the performance of services for the GN by including ownership clauses in favour of the GN in all contractual agreements. The next section provides a suggested wording for those clauses.

## 5. Things to Consider when Entering into Contractual Arrangements

The required elements for government contracts are established in the *Financial Administration Act,* the *Government Contract Regulations,* and the directives of the Financial Management Board. GN departments should consult with the Procurement and Purchasing Division of the Department of Community and Government Services and with legal counsel when entering into service contracts.

While this is not an exhaustive list, GN departments who are considering entering into contracts involving the collection, use, disclosure, storage, or destruction of personal information should consider:

- The GN and the contractor will both have obligations under the *ATIPP Act*, but does the contractor have to comply with any other access and privacy legislation? Are there any conflicts between legislative schemes? If in doubt, seek legal advice.

- Who will own the information created during the contract? Generally speaking, the GN owns the final report or product and any information that it supplied for the purposes of the contract.

- How will the information be transferred between the GN and the contractor? For example, will you send paper records by priority post, or will you use a secure file transfer protocol (FTP) system?

- What security and privacy protection measures does the GN require for this contract, and who is going to pay for them? The costs should be considered when developing your tender or proposal.

- Will the contractor be required to comply with industry best practices, such as the generally accepted privacy principles (GAPP)?

- Will the GN require the use of strong encryption and secure destruction?

- Will the GN want to inspect the contractor's facilities, or conduct a compliance audit during the life of the contract?

- Do you need to conduct a Privacy Impact Assessment (PIA) prior to entering into the contract?

- What happens to the information after the contract ends? Will it be returned to the GN, or will it be securely destroyed?

- How will the contractor respond to privacy incidents and breaches?

- If the contract is for research, have you met all the requirements of section 49 of the *ATIPP Act*? If you don't know, seek legal advice.

# Section 5:
# Privacy and the Management of Human Resources

## Contents

# 1. Information about GN Employees

The management of Human Resources (HR) involves the collection and creation of large volumes of personal information. This information is used for the management of programs such as recruitment and staffing, staff relations and employee assistance, as well as for the administration of employee benefits and to conduct statistical analysis and develop policies. An employee's personal information constitutes an important part of the GN's information holdings.

Whereas the *ATIPP Act* generally limits the use and disclosure of personal information about clients of public bodies and other individuals, it creates an exception in regard to the information that pertains to the professional status, roles, responsibilities and activities of GN employees, based on the premises that:

- Citizens should have the right to know who works for their government;
- they should be able to easily reach those employees when they need to; and
- the documents that are created by those employees in the course of employment are the property of the GN, not the employee's own personal property.

Consequently, all the information that relates to the position and which can be found in the job advertising poster, the working conditions associated with that position as well as everything that relates to the documentation that is created as part of the duties associated with that position can be used and disclosed by public bodies without the employees' consent or knowledge.

Of course, the above use and disclosure rule does not in any way apply to, or affect the confidentiality of the personal information that pertains more personally to the employee as a "person", such as:

- descriptions of an employee's skills, educational achievement, work experience, language level, and other details that reveal personal characteristics;
- information that pertains to the employee's personal life situation;
- financial information, such as income tax deductions, wage garnishing orders, pay deduction amounts, etc.;
- health-related information, including workplace accidents and worker's compensation reports;
- evaluative information;
- disciplinary information.

# 2. The Collection and Creation of Personal Information by Managers

The roles and responsibilities of managers expose them to a lot of personal information about employees, some of a very personal nature. The decision to transpose that information into a document depends on a number of factors, including (but not limited to):

- legal or policy requirements;

- its relevance and necessity for the administration of the GN's HR programs and related activities;
- the provision of advice or assistance to the employee;
- the desire of the employee to have it recorded or not.

Because the recording of that information makes it available for future use, and potentially hundreds of other individuals over the years to come, it must be limited to only those elements of information that absolutely need to be documented. It must also be done in a way that provides the entire context, and be supported by strong factual evidence. Ideally, the employee would be given an opportunity to review the information before the document is finalized and stored in a paper folder or an electronic system.

Of course, the challenge for managers resides in the determination of what should be documented, how it should be documented, and the degree of details to include in each document. The brochure titled "Creating Records in the Context of ATIPP" provides guidelines, advice and tips on how to document facts and opinions.

## 3. The Collection and Creation of Personal Information by HR Officers

Compared to managers, the creation and collection of information about employees by HR officers is generally done in a more formal context and must be done in accordance with clearly established processes. Also, it is often governed by policies and procedures, which minimizes the risk of capturing unnecessary information. HR officers are responsible for ensuring that only those elements of personal information that can legitimately be collected and created on behalf of the GN are included in an employee's paper and electronic files, that they are included in the right files, and that these elements of information are accurate, up-to-date and complete.

## 4. The Status of Managers' and Employees' Personal Notes under the ATIPP Act

Generally speaking, the records and information created and collected by managers and employees are considered the property of the GN if at least one of the following conditions applies:

- the individual created or collected the record or information in the course of the performance of his or her duties. On this, it must be noted that the notion of "duties" extends beyond the normal working hours of an employee and covers the whole 24 hour-7 day spectrum, irrespective of the fact that the manager or employee is producing the record or information during or outside normal business hours;

- the record or information pertains to the GN's mandate or activity. This excludes information of a personal nature that employees may create or collect during their working hours, such as personal shopping lists, personal emails sent to friends and family members, etc. unless the information also contains information pertaining to a work related activity; or

- the individual would not likely have created the record or information if he or she had not been working for the GN.

The notes and other statements created by managers about employees are subject to the *ATIPP Act* and, because employees have a right of access to them, their existence must be acknowledged openly. At the same time, they must be adequately protected from unauthorized access by other individuals as well as from unauthorized modification, use and/or destruction.

## 5. Background Checks

The conduct of background checks about candidates for employment has been designed to meet the requirements of section 8 of the *Canadian Charter of Rights and Freedoms* and the *ATIPP Act* by way of seeking the consent of the individual before the checks are conducted.

## 6. The Use and Disclosure of Personal Information about Employees

The *ATIPP Act* limits the use and disclosure of personal information to those situations that are described in sections 43, 47, 48 and 49. These circumstances fall under four broad categories:

**With the individual's consent:**

Consent refers to the individual giving "fully-informed consent"; this implies that the individual has clearly been made aware of all the possible ramifications that can result from the disclosure to enable him or her to make a sound decision. Ideally, those explanations would be provided on a written consent form, and a copy of the signed form would be given to the employee. The *ATIPP Act* only requires the consent to be in writing. An example would include the disclosure of an employee's personal information to an individual's legal counsel, union representative or financial institution. Another example is when an individual can't give his or her consent, and someone else is doing it for him or her for specific purposes. The executor of a will or the administrator of an estate, or someone with a power of attorney for property or personal care can consent on behalf of an individual who is unable to consent.

In all such cases, the disclosure must be limited to what these parties need to have in order to fulfill their obligations (administering the individual's estate, power of attorney, etc.) or commitment (grievance representation) to the individual.

All signed consent forms should be placed in the employee's file as a record of consent.

**For the purpose for which the personal information was originally created, collected or compiled or for a use consistent with the original purpose:**

Generally, this provision limits the uses and disclosures that can be made of an employee's personal information to only those purposes for which it was originally created or collected: background checks; *resumés* collected for one particular job competition; information provided for emergency situations, etc. The *ATIPP Act* allows for the collection, use and disclosure of personal information for the purpose of hiring and managing personnel.

The use of an employee's performance appraisal as a tool to assess that employee's suitability for a new position qualifies as a "consistent use" even though this is not the purpose for which such information was initially created. The key element is that if it is well prepared, a performance appraisal may constitute a very reliable measurement tool during the staffing process, as it highlights the employee's work-related strengths and weaknesses.

**In accordance with an enactment:**

The word "enactment" stands for act or regulation. This, for example, includes the disclosure of an employee's earnings information to the Canada Revenue Agency for the administration of the federal *Income Tax Act*, the *Employment Insurance Act* and corresponding territorial acts.

**For any of the special circumstances described in sections 48 and 49:**

Those circumstances include (but are not limited to):

- In response to a subpoena or court order;
- To an investigative body (under certain conditions);
- In the public interest;
- Where the disclosure would clearly benefit the individual to whom the information relates to, such as where an employee's personal information is disclosed to the next of kin in the context of an emergency situation;
- For research purposes – under strict conditions.

In all of those situations, the ATIPP coordinator should be consulted, because the delegated authority to make decisions in relation to these situations is often limited to certain individuals within GN public bodies.

## 7. Confidentiality within the Context of HR Management

**Staffing Process:**

The staffing process involves the collection of evaluative information about the job candidates, be it in the form of reference checks, the writing of notes by the members of the selection committee during the interview or the correction of the written tests that are sometimes administered. All of the information collected and created during the various steps of the staffing process is fully subject to the *ATIPP Act*, therefore, all individuals who participate in the process should be made aware that everything that they document can be requested by the candidates. No promise of confidentiality must ever be made to these individuals, and they must in fact be clearly told that the candidates may have the right to see their names when they appear with, or are associated to the comments that they have made about the candidates. In addition, all handwritten notes created during the staffing process must be kept even if their content have been transposed in a typed version to "official records", as these typed records may differ in substance and appearance from the original handwritten notes and, consequently, provide different contextual information.

## Administrative Investigation:

The expression “administrative investigation” encompasses a broad range of investigative activities such as those pertaining to harassment complaints, allegations of employee misconduct, security breaches, theft, fraud, workplace violence, grievances, workplace-related illnesses and accidents, etc.

The common denominator of all those investigative processes is that they involve the collection of information of a sensitive nature from witnesses and other available sources – experts, technical advisors, lawyers, IT administrators, etc., – as well as the production of reports, the making of administrative decisions and, sometimes, referrals to other entities such as the RCMP or an administrative tribunal. In some situations, where disclosure to law enforcement agencies could result in an individual facing criminal penalties, the GN should not release the information until presented with a court order, subpoena or search warrant.

The information collected during these processes is fully subject to the *ATIPP Act*, and the information collected can only be refused to an applicant if we can clearly establish with solid evidence that its disclosure at the time of the access request would jeopardize the ongoing investigation or compromise evidence that has not yet been collected and secured. Also, because the processing of an access request must normally be completed within 30 calendar days from the date of its receipt, we are not allowed to postpone the response to the applicant on the grounds that the investigation is ongoing or that management has not yet decided on the case.

Another important point: witnesses should be reminded at the beginning of each interview that confidentiality cannot be assured under any circumstances, and that everything that they say about other individuals and which gets recorded by the investigator will likely, in the eventuality that the case ends up in court, be disclosed to the parties involved in the case along with the witness’ identity. Such disclosures can also take place under the *ATIPP Act*. For these reasons, those who are mandated to conduct these investigations should clearly advise the witnesses to refrain from expressing exaggerated or false personal views and opinions including hearsay about other individuals, and they must only document such views and opinions when they are deemed to be highly relevant to the case.

Finally, all handwritten notes and other documents created or collected during the investigation process must be kept even if their content has been typed or incorporated into the investigation report, as these handwritten notes and other documents could be requested by the court or an administrative tribunal during a formal hearing process.

## Employee Assistance Program (EAP):

Individuals have a right under the *ATIPP Act* to request access to all views and opinions expressed about themselves by other individuals, EAP officers should document the views and opinions expressed by the employees who visit them regarding other individuals. EAP officers should also explain the other limitations to the confidentiality of exchanges at the beginning of each consultation, so that the employee is fully aware of the parameters of the EAP’s guarantee of confidentiality.

## 8. The Retention of Employees' Personal Information by Managers

A frequently asked question is the one pertaining to a manager's right or obligation to retain personal information about an employee outside of the official HR file – those sometimes referred to as shadow files. The answer is that this practice is acceptable provided that the retention is intended to support activities required to manage employees:

- monitoring attendance;
- preparing the employee's performance appraisal;
- supporting the development of a training or career plan;
- supporting the imposition of disciplinary measures;
- accommodating the employee's request to work from home;
- adjusting the working schedule;
- supporting a worker's compensation case.

It is also important to specify that proper storage and access controls must be used to ensure that the personal information is only accessible to those who have a legitimate need to see it. Also, the employees must be made aware of the existence of such information, so that they can exercise their right of access to it. Finally, a manager must not retain the information past the point where it is no longer needed at the local or branch level, in which case it must be transferred to the HR section responsible for the proper storage and retention of personnel records, or be disposed of in accordance with the GN's *Archives Act* and guidelines relating to the handling and disposal of transitory records.

## 9. Employees' Right to Request the Correction of their Respective Personal Information

In accordance with sections 45 and 46 of the *ATIPP Act*, individuals have a right to request the correction of any personal information about themselves which is under the control of a public body and, where a request for correction is received, the public body has the obligation to identify all other public bodies and third parties who were given access to that information during the last year, and it must send these parties a written notice to inform them that the individual to whom that information pertains is now contesting its validity.

Of course, public bodies can only fulfill their legal obligations in that respect if everyone who accesses such information systematically documents all their access to it and if all electronic repositories of such information are designed to keep track of these access activities.

Now, this does not mean that a record should be made of all activities performed by HR officers in regard to an employee's file. As part of their duties, it can reasonably be assumed that these employees will automatically become aware of any request for correction that may be presented in relation to the files they work with as this will be documented in those files. But an access record must be created for those individuals who have irregular access to those files, such as the members of a selection committee who look at the employee's performance appraisal during the staffing process.

# Section 6:
# Comprehensive Procedure for the Handling of Privacy Breaches and Incidents

## Table of Contents

# 1. Introduction

This comprehensive procedure for the handling of privacy breaches and incidents supports the GN's Privacy Breach Policy by providing detailed procedures to assist the ATIPP manager and the ATIPP coordinators for public bodies in identifying and responding to privacy incidents and privacy breaches and, where applicable, in investigating privacy breaches. It is complemented by the forms to be used to define and report privacy incidents and privacy breaches, and to facilitate the investigation of privacy breaches.

# 2. Objectives

These procedures aim to ensure that:

2.1 stakeholders, partners, contractors and other representatives of the GN are fully aware of their responsibilities as they relate to privacy incidents and privacy breaches;

2.2 privacy incidents and privacy breaches are quickly and properly identified/uncovered, reported, investigated and resolved;

2.3 harm to individuals that may result from privacy incidents and privacy breaches is avoided or mitigated;

2.4 concerns or questions about the impact of privacy incidents and privacy breaches on clients, employees and other affected individuals are addressed appropriately;

2.5 privacy inspections and privacy compliance audits are conducted in order to:

2.5.1 monitor the GN's privacy protection program;

2.5.2 prevent privacy incidents and privacy breaches;

2.5.3 verify that the GN programs, services and activities are conducted in compliance with the requirements of Part 2 of the *ATIPP Act* and the generally accepted privacy principles;

2.5.4 identify and address weaknesses in existing security measures;

2.5.5 identify and address weaknesses in existing and potential partnering and stakeholder relationships and agreements;

2.5.6 promote accountability;

2.5.7 identify the need, if any, for additional training.

## 3. Differentiating Privacy Incidents and Privacy Breaches

The consequences are essentially what differentiate a privacy incident from a privacy breach:

**Privacy incidents** can be quickly and easily corrected without any prejudice to the individual. They are usually resolved immediately by the employees who become aware of them.

**Privacy breaches**, on the other hand, may bring serious consequences for the individual and/or the GN, and they may require bold and comprehensive measures to minimize the damages. Consequently, they are the subject of systematic reporting and detailed response procedures.

Under Section 49.8 of the *ATIPP Act*, a privacy breach occurs with respect to personal information when there is unauthorized access or disclosure of information and/or loss of information which could result in information being accessed or disclosed without authority.

When a public body knows or has reason to believe that a breach of privacy has occurred with respect to personal information under its control the breach must be reported to the Information and Privacy Commissioner in accordance with Section 49.9 of the Act if the breach is *material*.

The factors that are relevant in determining whether a breach of privacy with respect to personal information under control of a public body is *material* include:

(a) the sensitivity of the personal information;
(b) the number of individuals whose personal information is involved;
(c) the likelihood of harm to the individuals whose personal information is involved; and
(d) an assessment by the public body of whether or not the cause of the breach is a systemic problem.

The report to the Information and Privacy Commissioner must be made as soon as reasonably possible after the public body knows or has reason to believe that the breach of privacy occurred and determines that the breach is *material*.

The individual affected must be notified of the breach of privacy if it is reasonable in the circumstances to believe that the breach of privacy creates a real risk of significant harm to the individual. The factors used to determine the risk of significant harm are listed under 49.10 (2) of the *ATIPP Act*.

Notification of others may be necessary if this action may reduce the risk of, or mitigate, any harm to the individual that could result from the breach of privacy, or a prescribed condition is satisfied.

The following tables provide guidance to help determine whether an event may be considered a privacy incident or a privacy breach.

| Privacy Incident and Privacy Breach Analysis Table 1 | | | |
|---|---|---|---|
| | **Circumstances** | **If the answer is "Yes"** | **If the answer is "No"** |
| **1** | Does the event seem to have occurred as a result of someone's deliberate action – such as a deliberate information leak, information theft, information destruction or sabotage of the information management system? | The event clearly qualifies as a privacy breach –it is most likely serious– and it requires an immediate and bold response. | It may still qualify as a privacy breach if the consequences for the individual(s), the public body and/or the GN are or may be serious – see the next table. Otherwise, it probably qualifies as a privacy incident. |

## Privacy Incident and Privacy Breach Analysis Table 2

Even if the event was not caused deliberately, it may still qualify as a privacy breach if the resulting consequences are serious for the individual(s), the public body and/or the GN or may be serious. The rows below offer some criteria to help in assessing the gravity factor.

| | Gravity of the Consequences | If the answer is "Yes" |
|---|---|---|
| **2** | Can someone's safety be compromised as a result of what happened? | It definitely qualifies as a privacy breach. |
| **3** | Is the event likely to have an adverse impact on the reputation of the public body or the GN? | It definitely qualifies as a privacy breach. |
| **4** | Is the event likely to have an adverse impact on the ability of the public body or the GN to conduct its activities or to deliver services to the public, such as:<br>• if the systems that are used to process data have been affected;<br>• if the information that is required for the activities has been los<br>• if the integrity of the information required for the activities has been altered (modified)?<br>• etc. | It definitely qualifies as a privacy breach. |
| **5** | Is the event likely to place the public body or the GN in a situation where it can be accused of having failed in terms of its legal or contractual obligations? | It definitely qualifies as a privacy breach. |
| **6** | Is the event likely to result in legal action being taken against the public body, the GN or another party? | It definitely qualifies as a privacy breach. |
| **7** | Is the event likely to generate media attention? | It may qualify as a privacy breach if the nature of the event is such that the public body or the GN would have to recognize publicly that:<br>• they failed to meet their legal or contractual obligations;<br>• the security measures in place were inappropriate or that the security rules were not complied with;<br>• the event is the result of gross negligence or a lack of due diligence. |
| **8** | Has a complaint been made to the Information and Privacy Commissioner for Nunavut or has the Commissioner informed the public body that an investigation would be conducted in relation to the event? | That does not in and by itself mean that the event qualifies as a privacy breach, but the public body should still conduct a full investigation to satisfy the request for information by the Commissioner. It may also have to take additional measures as suggested or recommended by the Commissioner. |

## 4. Preventing Privacy Incidents and Privacy Breaches

Privacy incidents and privacy breaches can primarily be prevented through the implementation of adequate safeguards and the conduct of privacy compliance inspections and privacy compliance audits. The inspection and audit processes are described in the *Procedure for the Conduct of Privacy Inspections and Privacy Compliance Audits* manual.

## 5. Responding to Privacy Incidents

Privacy incidents do not require the conduct of a full-scale investigation. Instead, employees must take immediate corrective action to resolve the incident, such as properly filing a misfiled record, stopping the decision-making process until all the relevant personal information is available or correcting personal information that is in error in the file. The ultimate objective is simple: to prevent any adverse consequence for the individual as well as for the GN.

Privacy incidents that seem to be systemic in nature must be reported to the ATIPP coordinator so that a comprehensive review may be conducted.

## 6. Responding to Privacy Breaches

**Stop the Breach:** take immediate action to prevent further invasion of privacy of all the individuals who are affected by the breach – e.g., put the files and records in a safe place, recover the lost documents, etc.;

**Limit the Harm:** take action to minimize the gravity of the consequences for the individuals who are affected by the breach – e.g., negotiating the return of the lost or stolen information to the GN, attempting to convince the individuals who have gained unauthorized access to the personal information to not use it, changing passwords that allow access to the data in the computers or systems, etc.;

**Document the Circumstances:** the circumstances of the breach must be fully documented using the form in Appendix 3.2;

**Investigate:** all allegations of privacy breaches, including acts of wrongdoing, security breaches and security violations that have privacy implications must be analysed by the ATIPP coordinator to determine if there are sufficient grounds to proceed with an investigation. There must be sufficient grounds and sufficient sources of evidence to prove or disprove the allegation. To make this determination, the ATIPP coordinator requests and gathers all relevant information about the circumstances of the privacy breach from all involved parties. If an investigation is required, the ATIPP coordinator conducts the investigation in accordance with sections 7 and 8, below. The ATIPP Coordinator within the public body will oversee the investigative process and report all findings to the ATIPP Manager. The ATIPP Manager will assist in determining whether the breach is material, and whether or not the Information and Privacy Commissioner or the individual to whom the information relates should be notified. All public body employees must cooperate fully with the investigation process and diligently provide all requested information.

Although the public body is responsible for their records and handling a privacy breach or incident, the Information Technology Division may be required to assist in the investigation process, given their administrative responsibility for information systems.

**Report the Investigation Results:** the Deputy Head will report the results of the investigation to the Head of the Public Body and the manager of the affected division or program unit. Where the breach presents a risk of legal action against the public body or a claim against the public body's insurance, the Deputy Head should also contact Legal Counsel of the Department of Justice and the Risk Management Division of the Department of Finance.

**Notify the Individual(s) Affected by the Breach:** The individual(s) affected must be notified of the breach of privacy if it is reasonable in the circumstances to believe that the breach of privacy creates a real risk of significant harm to the individual. The factors used to determine the risk of significant harm are listed under 49.10 (2) of the *ATIPP Act*. If it is judged that the breach may result in serious consequences from which individuals need to protect themselves, the quickest and most reliable means must be used to notify them. Assistance must be provided to the affected individuals to enable them to adequately protect themselves;

**Notify the Office of the Information and Privacy Commissioner of Nunavut:**
The ATIPP Manager, departmental ATIPP Coordinator and Legal Counsel (or a designated team), determine whether the breach is material, and provide a recommendation to the Deputy Head. In cases where the breach is material, the Deputy Head reports to the Information and Privacy Commissioner in accordance with Section 49.9 of the Act.

The factors that are relevant in determining whether a breach of privacy with respect to personal information under control of a public body is *material* are listed under 49.9 (2) and include:

(a) the sensitivity of the personal information;
(b) the number of individuals whose personal information is involved;
(c) the likelihood of harm to the individuals whose personal information is involved; and
(d) an assessment by the public body whether the cause of the breach is a systemic problem.

**Take other Appropriate Actions as Directed by the Circumstances:** take other actions as required, such as issuing a news release, contacting police forces, etc., as determined by the ATIPP manager in consultation with the Deputy Head, Legal Counsel, Risk Management and other relevant authorities. Corrective and preventative measures suggested or recommended by the Information and Privacy Commissioner will be given proper consideration.

# 7. Investigation of Privacy Breaches

## *7.1 Legislative, Regulatory and Policy Framework*

There are important human rights issues that must be considered during an investigation. The legislative, regulatory and policy framework includes (but is not limited to) the following authoritative documents:

- *Access to Information and Protection of Privacy Act*;
- *Canadian Charter of Rights and Freedoms*;
- *Canadian Human Rights Act*;
- *Financial Administration Act*;
- *Official Languages Act*;
- Departmental security policies and procedures;
- Applicable contractual arrangements – for contractors and other agents and representatives of the GN.

# 8. Procedure for the Investigation of Privacy Breaches

## *8.1 Importance of a Systematic Approach for the Conduct of Privacy Breach Investigations*

A privacy breach investigation is a systematic collection of information in any form and from all available sources to:

- reconstruct the facts that pertain to a real or suspected privacy breach;
- understand the causes and the effects of the situation;
- assess the gravity of the consequences resulting from the breach; and
- provide evidence that will support the decision-making process.

Because of the legal ramifications of investigations, it is essential that a systematic approach be used to ensure that:

8.1.1 all parties involved understand their respective roles and responsibilities and contribute positively to the process;

8.1.2 the rights of all parties involved in the process are respected at all times, in accordance with the due process principle and other applicable legal, regulatory and policy requirements;

8.1.3 all relevant aspects of the situation are thoroughly investigated;

8.1.4 all investigations are conducted in a consistent and appropriate manner;

8.1.5 the conclusions are based on demonstrable evidence and are adequately supported by well-established facts;

8.1.6 the results of all investigations are presented in a consistent manner;

8.1.7 the decisions that result from all investigations reflect the principles of fairness and dignity and that they are properly documented.

## *8.2 Step-by-Step Process for the Conduct of Privacy Breach Investigations*

All privacy breach investigations shall be conducted in accordance with this procedure.

### 8.2.1 Mandate and Terms of Reference

All allegations of privacy breaches, including acts of wrongdoing, security breaches and security violations that have privacy implications must be analyzed by the ATIPP coordinator to determine if there are sufficient grounds to conduct a full investigation. There must be sufficient grounds and sufficient sources of evidence to prove or disprove the allegation.

The ATIPP coordinator consults with the director/manager of the service or program where the privacy breach occurred, to appoint the investigator or determine the size and composition of the investigative team.

The mandate of the investigator/investigative team shall cover at least the following aspects:

8.2.1.1 purpose and scope of the investigation;

8.2.1.2 a clear and detailed statement of the allegations to be investigated/reviewed;

8.2.1.3 the powers and responsibilities of the investigator or investigative team;

8.2.1.4 the identity(ies) and title(s) of the investigator/investigative team and other individuals who are expected to participate in the process (i.e., IT or other experts who may have to be called to collect or analyze evidence, the witnesses, etc.);

8.2.1.5 a summary of the expected results – i.e. indication of the time frames within which the investigation is to be completed, the date by which the final report is required, the individuals to whom the report is to be presented, etc.);

8.2.1.6 an indication of the nature and extent of the resources and/or support available to the investigator/investigative team (clerical, technical, financial, legal, etc.);

8.2.1.7 any other specific instructions, such as the security measures to take when entering certain areas where sensitive information or assets are kept, how to report information about other types of illegal or inappropriate acts that are outside the investigation mandate, the receipt of information regarding the commission of criminal offences, etc.

### 8.2.2 Notifying the Respondent(s)

It is preferable not to notify the respondent(s) immediately in cases of privacy breaches that are alleged to have occurred as a result of wrongdoing, a deliberate security breach or security violation as this may jeopardize the investigation. The investigator/investigative team can wait until after the initial fact-finding phase is completed to notify the respondent(s), but it is recommended that this phase not be extended unduly. Once the risk of injury to the investigative process is lessened, the ATIPP coordinator will inform in writing the respondent(s) of the allegation(s) against them.

The *ATIPP Act* allows for an initial triage period to determine if the breach is material, and if the breach could cause significant harm to the individual. Once these determinations have been made, notification is mandatory.

### 8.2.3 Interviews

The investigator/investigative team is/are required to:

8.2.3.1 respect the constitutional and other rights of the individuals being interviewed;

8.2.3.2 inform the interviewees of their right to access, under relevant acts and court/adjudication procedures, any information about themselves which may be part of the investigation file;

8.2.3.3 inform the interviewees that everything they say about other individuals may have to be released to those individuals under certain acts, including the *ATIPP Act*, as well as in accordance with court or adjudication procedures;

8.2.3.4 afford the interviewees the opportunity to have a representative present during the interview, providing that the representative is not on the list of individuals to be interviewed at a later time;

8.2.3.5 ensure that any interviewee representative (union representative, lawyer, etc.) who is to be privy to sensitive information signs a written confidentiality undertaking;

8.2.3.6 refrain from discussing, revealing, or otherwise making available any information to anyone not authorized to be privy to any information about the investigation;

8.2.3.7 when possible, schedule interviews in writing, with notices to the immediate supervisor of the interviewee;

8.2.3.8 ensure that notes of all interviews are complete, understandable, legible, dated and in a form that makes them acceptable as evidence; and

8.2.3.9 place a copy of the interview notes in the privacy investigation file for retention according to the retention and disposition schedule established for those types of records.

### 8.2.4 The Investigation Report

A draft version of the investigation report must be submitted to the DM, ADM, director or manager of the service or program responsible for the area where the privacy breach occurred, as well as to all the other interested parties. Investigation reports should normally be structured as follows:

8.2.4.1 **Introduction: date of the report and summary of the allegation;**

8.2.4.2 **Findings:**

- detailed and chronological description of the facts;
- description of the evidence gathered – only hard/proven facts. No hypothesis or assumptions are to be included in this section of the report.

8.2.4.3 **Analysis:**

- explanation about the approach or methodology used to analyze the evidence collected;
- process by which the evidence was analyzed or assessed;
- statement explaining the investigator's assessment of the seriousness of the events and/or the rationale behind the investigator/investigative team's conclusions.

8.2.4.4 **Conclusion:**

- whether the allegation(s) is(are) founded or unfounded;
- what legal or regulatory requirements, standards, policy, etc., have been breached;
- statement indicating whether the allegation(s) is(are) supported or not by the evidence.

8.2.4.5 **Recommendations:**

- Recommendations may be made regarding the following aspects:
    - improvements to be made in relation to the existing programs, services, systems or practices;
    - training for the employees or contractors;
- No recommendations must be made by the investigator/investigative team in relation to sanctions to be imposed upon employees or contractors – because doing so would taint the objectivity of the investigation process.

8.2.4.6 **Signature by the investigator or the head of the investigation team.**

8.2.4.7 **Appendices:**

- Summary of Investigative Activities;
- Investigation Mandate (often referred to as Terms of Reference);
- Investigation Plan;
- Contributors to the Investigation Process;
- List of Interviewees;
- Witness Statements and Interview Notes;
- Investigators' Notes and other Documentary Evidence (e.g. certified copies of official documents or correspondence, newspaper articles, signed statements, transcripts of interviews, etc.);
- Other Appendices.

## Appendix 1 – Recommended Qualifications of External Resources for the Conduct of Privacy Compliance Audits and Privacy Breach Investigations

The following criteria aim to ensure that external resources (contractors) granted a contract to conduct privacy compliance audits and privacy breach investigations for the GN are properly qualified and that they possess a solid understanding of the mandate, operation and culture of the GN.

1. **Education and Privacy Work Experience:**

   a) A university degree in the arts, social sciences, law or public / business administration from a recognized university, **and** at least four years of continued experience in the privacy protection field within the last five years;

   **OR**

   b) High school diploma (or a General Equivalency Diploma) **and** at least five years of continued experience in the privacy protection field within the last six years.

2. **Formal Privacy Training:**

   Three days or more of formal privacy training by a credible / reputed organization should be considered an asset qualification.

3. **Experience in the Conduct of PIAs, Privacy Compliance Audits or Privacy Breach Investigations:**

   Experience acquired through the conduct of a combined total of at least ten (10) PIAs and / or privacy compliance audits and or privacy breach investigations during the last three years.

4. **Experience in the Analysis or the Development of Privacy Frameworks for Government Institutions:**

   a) Three years of experience in developing detailed, documented analyses of any Canadian jurisdiction's privacy framework, especially the GN *ATIPP Act*;

   **OR**

   b) Three years' experience in the development of privacy frameworks for a Canadian jurisdiction.

5. **Knowledge of the Mandate, Operation and Organizational Culture of the GN:**

   All candidates shall demonstrate a deep understanding of the mandate, operation and organizational culture of the GN.

**6. Privacy Experience in Other Canadian Jurisdictions:**

A wide range of experience in the privacy protection field with the provincial, territorial or municipal public sector or with First Nations governments, where that experience is consistent with the mandate, operation and culture of the GN, should be considered an asset qualification.

**7. Experience in the Security Field:**

An in-depth knowledge of security principles **and** who have conducted numerous security threat and risk assessments (TRA) for a Canadian jurisdiction should be considered an asset qualification, provided that candidates demonstrate a full understanding of the differences between:

a) security and privacy;

**AND**

b) the PIA and the TRA processes.

**8. Background in Investigation:**

The candidates must possess a combination of formal class training in investigation and interview techniques as well as a solid understanding of the principles of administrative law – due process, rights under the *Canadian Charter of Rights and Freedoms*, human rights legislation, etc. Four years of experience in the conduct of investigations in the fields of security, human rights, labour relations or harassment are considered an asset. Knowledge of the rules governing the criminal investigation process is also considered an asset.

## Appendix 2 – Forms and Templates

The following tables have been included as operational aids to facilitate resolution of a privacy breach.

## Appendix 2.1 – Statistical Report on Privacy Incidents and Privacy Breaches for Fiscal Year:

The table below is to be used by the ATIPP coordinators to document the statistical figures about the privacy breaches and incidents that are reported to that office during the fiscal year.

| | Nature of Privacy Incident or Privacy Breach Reported | Number of Privacy Incidents | Number of Privacy Breaches | Total Number of Individuals Affected | Total Number of Events Due to Error | Total Number of Events Due to Malicious Acts | Total Number of Events Due to Systems' Problems |
|---|---|---|---|---|---|---|---|
| 1 | Unauthorized collection of personal information. | | | | | | |
| 2 | Unauthorized use of personal information. | | | | | | |
| 3 | Unauthorized modification of personal information. | | | | | | |
| 4 | Inaccuracy of personal information. | | | | | | |
| 5 | Unauthorized disclosure of personal information. | | | | | | |
| 6 | Unauthorized retention of personal information. | | | | | | |
| 7 | Unauthorized destruction of personal information. | | | | | | |
| 8 | Unauthorized access to information management or communications systems. | | | | | | |
| 9 | Loss of personal information or asset that contained personal information. | | | | | | |
| 10 | Misfiling of personal information. | | | | | | |
| 11 | Others – please specify. | | | | | | |

| Response Measures to Privacy Incidents and Privacy Breaches | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Nature of Response Measures to the Reported Privacy Incidents and Privacy Breaches** | **Number of Privacy Incidents** | **Number of Privacy Breaches** | **Total Number of Individuals Affected** | **Total Number of Events Due to Error** | **Total Number of Events Due to Malicious Acts** | **Total Number of Events Due to Systems' Problems** |
| **1** | **Returned or destroyed the inappropriately collected personal information.** | | | | | | |
| **2** | **Stopped the unauthorized use of the personal information.** | | | | | | |
| **3** | **Reversed the unauthorized uses that were made of the personal information.** | | | | | | |
| **4** | **Reversed the unauthorized modifications that were made to the personal information.** | | | | | | |
| **5** | **Corrected the inaccurate personal information.** | | | | | | |
| **6** | **Informed all the parties who have been provided access to, or allowed to use the inaccurate personal information of the error.** | | | | | | |
| **7** | **Recovered the personal information that was disclosed inappropriately.** | | | | | | |
| **8** | **Had the personal information that was inappropriately disclosed destroyed.** | | | | | | |
| **9** | **Disposed of the personal information that was inappropriately retained beyond its approved retention period.** | | | | | | |
| **10** | **Recovered the personal information that was destroyed.** | | | | | | |
| **11** | **Stopped the unauthorized access to the information management or** | | | | | | |

| Response Measures to Privacy Incidents and Privacy Breaches | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Nature of Response Measures to the Reported Privacy Incidents and Privacy Breaches** | **Number of Privacy Incidents** | **Number of Privacy Breaches** | **Total Number of Individuals Affected** | **Total Number of Events Due to Error** | **Total Number of Events Due to Malicious Acts** | **Total Number of Events Due to Systems' Problems** |
| | **communications system.** | | | | | | |
| **12** | **Recovered the lost personal information or the lost asset that contained personal information.** | | | | | | |
| **13** | **Properly filed the misfiled personal information.** | | | | | | |
| **14** | **Unsuccessfully attempted to take one or several of the above measures.** | | | | | | |
| **15** | **Referred the case to a law enforcement agency.** | | | | | | |
| **16** | **Informed the individual(s) whose personal information or privacy rights were compromised.** | | | | | | |
| **17** | **Provided other form of assistance to the individual(s) whose personal information or privacy rights were compromised.** | | | | | | |
| **18** | **Informed the Information and Privacy Commissioner.** | | | | | | |
| **19** | **Issued a public statement to inform all interested individuals across the Territory and, where applicable, Canada, of the privacy incident or the privacy breach.** | | | | | | |
| **20** | **Others – please specify.** | | | | | | |

## Appendix 2.2 – Privacy Incident / Privacy Breach Report

| Status as a Privacy Incident or Privacy Breach<br>(Please provide rationale and append all the relevant documentation to this report.) | | |
|---|---|---|
| 1 | Date of the report. | |
| 2 | Author(s) of the report. | |
| 3 | Contact information for the author(s) of the report. | |

| Status as a Privacy Incident or a Privacy Breach<br>(Please provide rationale and append all the relevant documentation to this report) | | |
|---|---|---|
| 5 | Privacy Incident | Privacy Breach |
| 6 | | |

| Nature of the Privacy Incident or the Privacy Breach<br>(for statistical purposes) | | |
|---|---|---|
| 7 | ☐ Unauthorized collection of personal information<br>☐ Unauthorized use of personal information<br>☐ Unauthorized modification of personal information<br>☐ Inaccuracy of personal information<br>☐ Unauthorized disclosure of personal information<br>☐ Unauthorized retention of personal information<br>☐ Unauthorized destruction of personal information | ☐ Unauthorized access to information management or communications system<br>☐ Loss of personal information of personal information or asset that contained personal information<br>☐ Misfiling of personal information<br>☐ Other – please specify: |

| Details of the Privacy Incident or the Privacy Breach | | | |
|---|---|---|---|
| | **Reporting Criteria** | **Comments and Observations** | **Response or Comments from (insert TITLE) and/or the ATIPP coordinator** |
| **8** | Known or approximate dates of the incident or breach. If the exact dates are not known, please explain why. | | |
| **9** | Time that it took to discover the privacy incident or the privacy breach. | | |
| **10** | Circumstances that lead to the discovery of the privacy incident or the privacy breach. | | |
| **11** | Individual(s) or segment(s) of the population whose privacy rights were affected by the event. | | |
| **12** | Categories of personal information that was compromised. | | |
| **13** | Circumstances surrounding the privacy incident or the privacy breach. | | |
| **14** | Real or anticipated consequences of the privacy incident or the privacy breach. | | |
| **15** | Measures that have been / are being taken to minimize the consequences of the compromise. | | |
| **16** | Have the individuals whose privacy has been compromised been notified? If so, please explain how and why that method was used.<br><br>If no, please provide the rationale for the decision. | | |
| **17** | Other relevant information. | | |

| Parties involved in the Incident and Who Can Provide information about the Event | | |
|---|---|---|
| | **Names** | **Titles and Coordinates** |
| **18** | | |
| **19** | | |
| **20** | | |
| **21** | | |

| Signature Block | | |
|---|---|---|
| **22** | _____<br>Signature of Head of Responsibility Centre | _____<br>Signature of ATIPP coordinator |
| **23** | _____<br>Signature of (TITLE) | _____ |
| This form last revised May, 2013 | | |

## Appendix 2.3 – Privacy Incident / Privacy Breach Investigation Report

| Status as a Privacy Incident or Privacy Breach<br>(Please provide rationale and append all the relevant documentation to this report.) | | |
|---|---|---|
| 1 | Date of the report. | |
| 2 | Author(s) of the report. | |
| 3 | Contact information for the author(s) of the report. | |

| Status as a Privacy Incident or a Privacy Breach<br>(Please provide rationale and append all the relevant documentation to this report) | | |
|---|---|---|
| 5 | Privacy Incident | Privacy Breach |
| 6 | | |

| Nature of the Privacy Incident or the Privacy Breach<br>(for statistical purposes) | | |
|---|---|---|
| 7 | ☐ Unauthorized collection of personal information<br>☐ Unauthorized use of personal information<br>☐ Unauthorized modification of personal information<br>☐ Inaccuracy of personal information<br>☐ Unauthorized disclosure of personal information<br>☐ Unauthorized retention of personal information<br>☐ Unauthorized destruction of personal information | ☐ Unauthorized access to information management or communications systems<br>☐ Loss of personal information of personal information or asset that contained personal information<br>☐ Misfiling of personal information<br>☐ Other – please specify: |

| Details of the Privacy Incident or the Privacy Breach | | | |
|---|---|---|---|
| | **Reporting Criteria** | **Comments and Observations** | **Response or Comments from the ATIPP coordinator** |
| **8** | Known or approximate dates of the incident or breach. If the exact dates are not known, please explain why. | | |
| **9** | Time that it took to discover the privacy incident or the privacy breach. | | |
| **10** | Circumstances that lead to the discovery of the privacy incident or the privacy breach. | | |
| **11** | Individual(s) or segment(s) of the population whose privacy rights were affected by the event. | | |
| **12** | Categories of personal information that were compromised. | | |
| **13** | Circumstances surrounding the privacy incident or the privacy breach. | | |
| **14** | Real or apprehended consequences of the privacy incident or the privacy breach. | | |
| **15** | Measures that have been/are being taken to minimize the consequences of the compromise. | | |
| **16** | Have the individuals whose privacy has been compromised been notified? If so, please explain how and why that method was used.<br><br>If no, please provide the rationale for the decision. | | |

| Narrative Section | |
|---|---|
| 17 | **Introduction** |
| 18 | **Allegation** |
| 19 | **Background / Context of Allegation** |
| 20 | **Approach and Methodology for the Conduct of the Investigation** |
| 21 | **Findings** |
| 22 | **Conclusion(s)** |
| 23 | **Recommendations** |

| Signature Block | | |
|---|---|---|
| 24 | _____<br>Signature of Main Investigator | _____<br>Signature of ATIPP coordinator |
| 25 | _____<br>Signature of TITLE | _____ |

This form last revised December 31, 2012

## Report Appendix 1 Summary of Investigative Activities

| | Activities | Dates | Observations |
|---|---|---|---|
| **1** | Beginning of the investigation | | |
| **2** | • Preliminary gathering of information<br>• Preparation of investigation plan<br>• Drafting of letters to invite witnesses to interviews<br>• Preliminary identification of witnesses | | |
| **3** | Appointments scheduled and convocation letters sent to the witnesses | | |
| **4** | Interviews with witnesses | | |
| **5** | Other activities | | |
| **6** | Submission of interim report | | |
| **7** | Comments received from the interested parties | | |
| **8** | Writing of final investigation report | | |
| **9** | Submission of final investigation report | | |

**Report Appendix 2 – Example of an Investigation Mandate**

A regional administrative investigation team has been established under the authority of (insert name and title of person with authority to mandate an investigation), to examine allegations of (matter) against (insert name and title of individual).

The team is to undertake the following:

- investigate (matter);
- investigate any other related issues that may be disclosed during the course of the investigation;
- determine whether any misconduct occurred and, if it did, whether any mitigating factors existed;
- submit a written report of its findings to (name and title of person who mandated investigation) by (date); and
- the investigation will be conducted in accordance with the GN Privacy Breach and Incident Policy.

The team will be composed of:

(Insert Names and Titles of Team Members)

The team is to be allowed access to all relevant departmental documents as deemed necessary. The team may interview such persons as it deems appropriate. At the commencement of the interviews, the committee will inform the employees of their rights and obligations under the *Access to Information and Protection of Privacy (ATIPP) Act*, and will ensure that the employees understand their rights and obligations with respect to confidentiality and representation at interviews. Any such employees will be authorized time off with pay to appear before the team.

All costs related to the investigation will be paid by (insert name of department/division).

The team is to report its findings to the undersigned as soon as possible, but not later than (date).

Regional contact is (insert name and title of regional contact). Administrative support will be provided by (insert name and title of administrative support / or name of division).

_____ _____

(Signature of Person mandating investigation) (Date)

## Report Appendix 3 – Example of an Investigation Plan

| Activity | Date | Comments |
|---|---|---|
| Beginning of the investigation | | This is the date on which the investigation mandate is signed |
| • Preliminary gathering of information<br>• Preparation of investigation plan<br>• Drafting of letters to invite witnesses to interviews<br>• Preliminary identification of witnesses | | |
| Appointments scheduled and convocation letters sent to the witnesses | | |
| Interviews with witnesses | | As per accompanying list of interviewees |
| Submission of preliminary investigation interim report | | |
| Comments received from department on the interim investigation report | | |
| Writing of final investigation report | | |
| Submission of final investigation report | | |

## Report Appendix 4 – Contributors to the Investigation Process

| | Names | Titles and Coordinates |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

## Report Appendix 5 – Interviewees

| | Names | Titles and Coordinates |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

## Report Appendix 6 – Witness Statements and Interview Notes

**Name of Interviewee:**

**Status of Interviewee:**
(employee, contractor, client, etc.)

**Title:**
(for employees)**:**

**Place of work:**
(for employees and contractors)

**Date of interview:**

**Time of interview:**

**Place of interview:**

**Purpose of interview:**

**Summary of interview:**

Report facts and other information as provided by the witness – from the interview notes

## Report Appendix 7 – Investigators' Notes and other Documentary Evidence

| | Description of Appended Document or Description and Location of Other Type of Object Used as Evidence |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |

## Report Appendix 8 – Other Relevant Documents

| | Description of Appended Document |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |

# Section 7:
# Comprehensive Procedure for the Conduct of Privacy Impact Assessments

## Table of Contents

# Table of Appendices

# 1. Introduction

This document supports the GN's Privacy Policy by providing a detailed procedure for the conduct of Privacy Impact Assessments (PIA). It is accompanied by forms and other tools that are designed to facilitate the conduct of PIAs.

# 2. Effective Date

This procedure takes effect on (insert date).

# 3. Objectives of PIAs

PIAs aim to ensure that all the initiatives that may have an adverse impact on the privacy of individuals are properly examined to ensure that they are designed and administered in accordance with the requirements of the *ATIPP Act* and the "generally accepted privacy principles". In this context the term "initiative" encompasses:

3.1.1. the adoption of a new policy, process or procedure that affects how personal information is collected, used, shared/disclosed, stored, transmitted, protected or disposed of;

3.1.2. a significant change made to an existing policy, process or procedure that affects how personal information is collected, used, shared/disclosed, stored, transmitted, protected or disposed of;

3.1.3. the acquisition of a new information management or communications system that affects how personal information is collected, used, shared/disclosed, stored, transmitted, protected or disposed of;

3.1.4. the collection of new categories of personal information or the collection of personal information about new categories of individuals;

3.1.5. any other activity that may in any way affect the privacy rights of individuals.

# 4. Importance of a Systematic Approach for the Conduct of PIAs

A systematic approach is required to ensure that:

4.1.1. the parties involved are fully aware of, and understand their respective roles and responsibilities and contribute positively to the process;

4.1.2. PIAs are conducted in a consistent manner throughout the GN; and

4.1.3. all approved recommendations are implemented in a timely and cost-effective manner.

# 5. PIA Process

## 5.1 Steps in the Conduct of a PIA

Generally, a PIA is comprised of the following steps:

### Step One – Initiation

5.1.1. Project authorities must determine whether a PIA needs to be conducted in relation to each new initiative that falls under their responsibility. This is done by completing the **Summary of Initiative Description to Determine the Need for a Privacy Impact Assessment** form at Appendix 2 and the **Risk Area Identification and Categorization Table** at Appendix 3.

5.1.2. Where the assessment leads to the conclusion that a PIA is required, the ATIPP coordinator and the project authority jointly appoint a PIA team – which may consist of one or more individuals, depending upon the magnitude and complexity of the PIA;

5.1.3. The PIA team must:

- determine the scope and timeline of the PIA;
- decide on the approach for the collection of the required information;
- identify the relevant information sources – individuals to interview, required documentation, etc.;
- develop or adapt the PIA tools – questionnaires and analysis tables at Appendices 4 – as required;
- assign tasks to each team member;
- send notices to the responsibility centres and other parties to inform them of the conduct of the PIA and to seek their cooperation.

### Step Two – Information Collection

5.1.4. The PIA team proceeds with the collection of the information required for the assessment, using the analysis tables at Appendix 4.

5.1.5. The team must ensure that:

- all contributors to the PIA process are educated about the privacy concept, the requirements of the *ATIPP Act* as they relate to privacy protection as well as with the "generally accepted privacy principles" – failing to adequately explain the privacy concept to these contributors at the beginning of the PIA process will invariably lead to confusion and increase the risk that key aspects of the initiative be missed;

- the information received from the various parties is complete, accurate and up-to-date – this is particularly important for off-the-shelf computer applications which are modified to suit the specific requirements of the GN because the descriptive documents and the users manuals may only reflect the characteristics of the generic version;

- the sensitive information, such as the security features, that it receives about the program, functions, activities or system is adequately safeguarded against unauthorized access, modification and destruction.

## Step Three – Analysis

5.1.6. The first phase of the analysis consists of acquiring a full understanding of the program, function, activity or system for which the PIA is being done. This is the most challenging phase of the PIA process because it usually involves highly technical information and, because the project is in most cases still under development, the parameters keep changing. Consequently, the PIA team must constantly validate the information with the sources and/or subject matter experts. The PIA team should try to obtain valuable documents such as "CONOP" (Concept of Operation), user's manuals for information management systems, security threat and risk assessment (TRA) reports, design manuals containing graphical representations of the systems and narrative explanations, etc.;

5.1.7. The second phase addresses the privacy risks associated with the initiative and entails a detailed review of the following aspects of the initiative:

- the legal or other authority for the collection, use, sharing/disclosure, retention and disposition of the personal information involved;

- the risks associated with the design and operation of the new or modified policy, process, procedure or system;

- the risks associated with the collection, use, sharing/disclosure, retention and disposition of the personal information involved;

- the measures in place to protect the personal information from unauthorized collection, use, access, modification and destruction;

- the general privacy related risks posed by the initiative:

- how it will change the nature of the relationship between the public body and its clients, employees and members of the public;

- whether the initiative is likely to affect the reputation, safety or life opportunities of certain individuals;

- whether the policies, procedures and training programs in place within the public body provide adequate safeguards against an unreasonable invasion of privacy;

- in those cases where the initiative involves an information-sharing program or a contract with a private entity, an analysis of the terms of the contractual agreement and the privacy policies of all the parties involved is needed to ensure that they satisfy the requirements of the GN;

- finally, the public and media repercussions of the initiative to determine whether a communications plan should be developed.

## Step Four – PIA Report

5.1.8. A PIA report must normally contain:

- a narrative description of the scope and methodology used for the PIA. This includes a description of the criteria that were used to perform the assessment in regard to each of the following aspects:

    - creation/collection;
    - use;
    - disclosure;
    - accuracy and integrity;
    - retention and disposition;
    - safeguarding – administrative, physical and technical;
    - where applicable, the information exchange agreement, including the legislative and policy framework applicable to each party involved in the agreement and the privacy and security policies of each party involved in the agreement;

- individuals' consent, access and correction rights;

- a plain language narrative description of the program, function, activity or system for which the PIA is being conducted, including the technology, the procedures and the processes;

- a narrative description of the benefits of the initiative;

- a narrative description of the findings in relation to each of the privacy and security criteria used for the assessment;

- graphical representations or tables showing the information flows associated with the program, function, activity or system;

- a summary of the legal opinions that may have been obtained during the PIA;

- where applicable, the need for the GN to inform the interested segment(s) of communities of the new initiative and its privacy related implications;

- where applicable, the options, suggestions and recommendations, based on the table at Appendix 6;

- where possible, a proposed time frame for the implementation of the recommendations, and an estimate of the costs associated with their implementation;

- as an appendix to the report, the Summary of PIA Findings table, which can be found at Appendix 5;

- any other relevant information.

The completed analysis tables from Appendices 2, 3 and 4 may be appended to the report where necessary to support the findings or recommendations.

## Step Five – Validation and Approval of the PIA Report

5.1.9. Before finalizing the PIA report, the project authority must submit copies of it to all the parties who have a direct interest in the program or activity.

## Step Six – Follow-up and Monitoring

5.1.10. The ATIPP coordinator is responsible for monitoring the implementation of the approved recommendations.

# Table of Appendices

# Appendix 1 – Recommended Qualifications of External Resources for the Conduct of PIAs

The following criteria aim to ensure that the external resources (contractors) who are granted a contract to conduct PIAs for the GN are properly qualified and that they possess a solid understanding of the mandate, operation and culture of the GN. These criteria are consistent with those required by several other Canadian jurisdictions.

**9. Education and Privacy Work Experience:**

c) A university degree in the arts, social sciences, law or public / business administration from a recognized university, **and** at least four years of continued experience in the privacy protection field within the last five years;

**OR**

d) High school diploma (or a General Equivalency Diploma), **and** at least five years of continued experience in the privacy protection field within the last six years.

**10. Formal Class Privacy Training:**

Although not a common requirement, the candidates who have attended at least three days or more of formal privacy training by a reputable organization should be granted more evaluation points in the scoring grid.

**11. Experience in the Conduct of PIAs or Privacy Compliance Audits:**

Experience acquired through the conduct of a combined total of at least ten (10) PIAs and / or privacy compliance audits during the last three years.

**12. Knowledge of the Mandate, Operation and Organizational Culture of the GN and Nunavut Communities:**

All candidates shall demonstrate a thorough understanding of the mandate, operations and organizational culture of the GN and Nunavut communities.

**13. Privacy Experience in Other Canadian Jurisdictions:**

The candidates who can demonstrate a wide range of experience in the privacy protection field with the provincial, territorial or municipal public sector or with First Nations governments may be granted equivalency points in the scoring grid, provided that their experience is consistent with the mandate, operations and culture of the GN and Nunavut communities.

**14. Experience in the Security Field:**

The candidates who possess an in-depth knowledge of information security **and** who have

conducted numerous security threat and risk assessments (TRA) should be granted equivalency points in the scoring grid, provided that they can demonstrate a full understanding of the differences between:

c) security and privacy;

**AND**

d) the PIA and the TRA processes.

## Appendix 2 – Summary of Initiative Description to Determine the Need for a Privacy Impact Assessment

| | | |
|---|---|---|
| **Government of Nunavut**<br><br>_____<br>**(Name of Public Body)**<br>**Summary of Initiative Description to Determine the Need to Conduct a Privacy Impact Assessment** | | |
| **Section A – To Be Completed by the Initiative Authority** | | |
| **1** | Date | |
| **2** | Title/name of the initiative – and acronym. | |
| **3** | Project Authority – the primary entity responsible for the initiative. | |
| **4** | Name and contact information of the individual who is responsible for coordinating the initiative. | |
| **5** | Planned commencement date. | |
| **6** | Estimated duration. | |
| **7** | Purpose of the initiative. | |
| **8** | Legal/policy authority for the initiative. | |

| | | |
|---|---|---|
| **9** | Description of the initiative, including the development and implementation phases. | |
| **10** | Anticipated result and success criteria. | |
| **11** | Description of the categories of personal information that will be involved in the initiative. | |
| **12** | How will the initiative change the current practices of the GN or public body. | |
| **13** | Segments of the population who will likely be affected by the initiative. | |
| **14** | Why personal information will have to be involved. | |
| **15** | How the privacy of individuals may be adversely affected by the initiative. | |
| **16** | Whether the initiative has been announced or not to the community. If not, explain why. | |
| **17** | Identify all the parties that need to be involved in the initiative – from within and outside the GN or public body. | |
| **18** | The budget allocated for the initiative. | |

| | | |
|---|---|---|
| **19** | Any other relevant information. | |
| **20** | Has a security threat and risk assessment been conducted in relation to the initiative? | |
| **21** | Project authority's observations. | |
| **Section B – To Be Completed by the ATIPP Coordinator** | | |
| **22** | Is a PIA required for this initiative? (provide rationale for decision) | |
| **Section C – Signature Block** | | |
| **23** | _____<br>Signature of Project uthority | |
| This form last revised May 2013 | | |

# Appendix 3 – Risk Area Identification and Categorization Table

The following table is used to determine:

- the scope of the PIA;
- the need for legal opinions on various aspects of the initiative;
- the need for a communications strategy, and, if so, its approach, the level of detail and its target population;
- the scope and nature of the privacy protection and security measures to be implemented as well as the mitigation measures to address the residual risks; and
- any other relevant aspect.

| | Factor / Criteria | Risk scale | Actual Assessment |
|---|---|---|---|
| **1** | Program or activity that does NOT involve the use of personal information to make decisions about identifiable individuals – e.g., the collection of statistical information, the review of individual files for program evaluation. | 1 | N/A |
| **2** | Administration of program or activity and general services to the community that involve low-sensitive personal information – e.g., mailing lists for pamphlets, invitations to social activities. | 2 | N/A |
| **3** | Information exchange agreement with an outside party (government institution or private sector organization) that involves low-sensitive personal information, such as one that is limited to the sharing of names and addresses. | 2 | N/A |
| **4** | Commercial activities in a competitive environment – e.g., client lists, vendor identification and assessment, evaluation of products and services. | 3 | N/A |
| **5** | Compliance audits, regulatory investigations and enforcement of policies and procedures – administrative investigation, interviews conducted during compliance audits, traffic violations, and non-serious offences. | 4 | N/A |
| **6** | Information exchange agreement with an outside party (government institution or private sector organization) that involves medium-sensitive personal information, such as work-performance-related and financial information. | 4 | N/A |
| **7** | Criminal investigation, law enforcement and safety of individuals, including family violence and child protection. | 5 | N/A |

| | Factor / Criteria | Risk scale | Actual Assessment |
|---|---|---|---|
| **8** | Provision of physical or mental health care services or other social services that involve sensitive personal information about identifiable individuals. | 5 | Applicable |
| **9** | Information exchange agreement with an outside party (government institution or private sector organization) that involves highly-sensitive personal information, such as health or criminal record information. | 5 | Applicable |

# Appendix 4 – Privacy Impact Assessment Privacy Analysis Tables

**IMPORTANT NOTE:**

The Privacy Analysis Tables on the following pages are designed to guide the information collection and analysis processes for a wide range of PIAs. Some, such as those that pertain to information exchange agreements, are relevant to only certain types of PIA. Where applicable, they should be adapted/modified to suit the particulars of each type of initiatives that result or may result in a change to any policy, process, system or procedure for which a PIA is conducted.

When using the Privacy Analysis Tables it is important to remember that the goal is to use them for a rigorous analysis of the characteristics of the initiative so that those that present a potential invasion of privacy are identified and properly addressed.

# Annex 4.1 – Elements of Personal Information Involved in the Initiative

| Privacy Analysis Table 4.1<br>Elements of Personal Information Involved in the Initiative | | | |
|---|---|---|---|
| | **Elements of Personal Information to Be Collected** | **Sub-elements of Personal Information (e.g., for an individual's name, the sub-elements of PI include the first name, aliases, etc.)** | **Reason for the Collection** |
| **1** | | | |
| **2** | | | |
| **3** | | | |
| **4** | | | |
| **5** | | | |
| **6** | | | |
| **7** | | | |
| **8** | | | |
| **9** | | | |
| **10** | | | |
| **11** | | | |
| This form last revised: May 2013 | | | |

## Annex 4.2 – Privacy Analysis Table 2 – Collection

| Privacy Analysis Table 4.2<br>Collection | | | |
|---|---|---|---|
| | **Criteria** | **Assessment** | **Observations** |
| **1** | Legal, regulatory or policy authority for the collection. | | |
| **2** | Specify whether the collection is required or just authorized by law, a regulation or a policy. | | |
| **3** | Describe the avenues that have been explored to achieve the legislative or operational objectives without collecting personal information. | | |
| **4** | Specify whether the collection of personal information will be direct or indirect and provide rationale. | | |
| **5** | Collection method. | | |
| **6** | Notice provided to individuals – describe how notice is provided (written, verbal, etc.) and whether it covers the following aspects:<br>• the purpose of the collection;<br>• whether response is voluntary or required by law;<br>• any possible consequences that may result from the individual's refusal to provide the requested information;<br>• that the individual to whom the information pertains has rights of access to and protection of the personal information under the *ATIPP Act*. | | |
| **7** | Describe how consent is obtained from the individuals to whom the personal information pertains. | | |

| Privacy Analysis Table 4.2<br>Collection | | | |
|---|---|---|---|
| | **Criteria** | **Assessment** | **Observations** |
| **8** | Risks associated with the collection – the fact that the information is collected, the method used for the collection, the context of the collection, the risks for the sources offering the information and for the employees who receive it, the possibility of a legal challenge, etc. | | |
| This form last revised: May 2013 | | | |

## Annex 4.3 – Privacy Analysis Table 3 – Use

| Privacy Analysis Table 3<br>Use | | | |
|---|---|---|---|
| | **Criteria** | **Assessment** | **Observations** |
| **1** | Description of the uses that are intended to be made of the personal information – primary and secondary. | | |
| **2** | Where applicable, explain whether the secondary uses qualify as "consistent uses". | | |
| **3** | Legal authority for the primary and secondary uses. | | |
| **4** | Specify whether or not the individuals to whom the personal information pertains are made aware of all the intended and real uses. | | |
| **5** | Whether consent should be/has been obtained from the individuals to whom the personal information pertains regarding the uses. | | |
| **6** | Specify how many individuals will be using the personal information and for what purposes – describe the criteria that have been used to identify these authorized users. | | |
| **7** | Describe the physical or electronic environment in which the personal information will be used – protected, public, etc. | | |
| **8** | Describe how the personal information will circulate among the users – i.e., information flows. | | |
| **9** | Risks associated with the uses – the fact that the information is being used for the intended and secondary purposes (consistent uses), the environmental and electronic conditions of the uses, the risks for the users and individuals to whom the personal information pertains, possibility of a legal challenge, etc. | | |
| This form last revised: May 2013 | | | |

## Annex 4.4 – Privacy Analysis Table 4 – Disclosure

Where applicable, this table is to be used in conjunction with the Privacy Analysis Tables at Annexes 5, 6 and/or 7.

| Privacy Analysis Table 4.4<br>Disclosure | | | |
|---|---|---|---|
| | **Criteria** | **Assessment** | **Observations** |
| **1** | Description of the disclosures that are intended to be made of the personal information – primary and secondary. | | |
| **2** | Where applicable, explain whether the secondary disclosures qualify as "consistent uses" or fall under another provision of the ATIPP Act. | | |
| **3** | Legal, regulatory or policy authority for the primary and secondary disclosures. | | |
| **4** | Specify whether or not the individuals to whom the personal information pertains are made aware of all the disclosures. | | |
| **5** | Whether consent should/has been obtained from the individuals to whom the personal information pertains regarding the disclosures. | | |
| **6** | Identify all the parties to whom the personal information will be disclosed – describe the criteria that have been used to identify the authorized users. Where applicable, use the Privacy Analysis Tables at Annexes 5, 6 and/or 7 to analyze the information sharing agreements. | | |
| **7** | Describe all the uses that the receiving parties will make of the personal information. | | |
| **8** | Describe the environmental and electronic conditions in which the personal information will be disclosed. | | |

| Privacy Analysis Table 4.4<br>Disclosure | | | |
|---|---|---|---|
| | **Criteria** | **Assessment** | **Observations** |
| **9** | Describe how the personal information will circulate among the users – i.e., information flows – and include graphical representations in the narrative part of the PIA report. | | |
| **10** | Risks associated with the disclosures – the fact that the information is being disclosed for the intended and secondary purposes, the environmental and electronic conditions of the disclosures, the risks for the parties involved in the exchange and individuals to whom the personal information pertains, possibility of a legal challenge, etc. | | |
| This form last revised: May 2013 | | | |

# Annex 4.5 – Privacy Analysis Table 5 – Privacy Analysis of a Personal Information Exchange Agreement between the GN and another Government Organization

This table is to be used in conjunction with Table 4.4 for the analysis of an information exchange agreement between the GN and another government organization.

| Privacy Analysis Table 5<br>Privacy Analysis of a Personal Information Exchange Agreement between the GN and another Government Organization<br>(Federal, Provincial, Territorial, Inuit Organization or Foreign) | | | | |
|---|---|---|---|---|
| | **The Agreement Should…** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **General Terms of the Agreement** | | | | |
| **1** | Specify, in clear terms, the purpose of the agreement. | | | |
| **2** | Clearly identify the parties to the agreement - by their legal names or identifiers. Where the agreement is signed by a component of an organization (directorate, branch, etc.), the name of that component must be specified in the agreement. | | | |
| **3** | Specify the titles of the individuals in each participating organization who are responsible for ensuring compliance with the terms of the agreement. | | | |
| **4** | Clearly identify the legal, regulatory or policy authority that allows or requires the GN or public body to enter into the agreement. | | | |
| **5** | Clearly identify the legal, regulatory or policy authority for the other party to enter into the agreement with the GN or public body. | | | |
| **6** | Specify the duration of the agreement, and the amendment procedure. | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Personal Information Exchange Agreement between the GN and another Government Organization (Federal, Provincial, Territorial, Inuit Organization or Foreign) | | | | |
|---|---|---|---|---|
| | **The Agreement Should…** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **7** | Specify the process by which the parties can terminate the agreement before the negotiated expiry date. | | | |
| **8** | Specify the responsibilities of each party as they relate to the identification of security and privacy breaches, the reporting of such breaches to the other party, the investigation of those breaches and how the situations are to be addressed – i.e., who informs the individuals whose personal information has been compromised, how this is done, etc. | | | |
| **9** | Identify the legal jurisdiction whose laws shall prevail in case of a disagreement or conflict pertaining to the agreement. | | | |
| **10** | Protect each party from the consequences of court actions taken against the other one, and specify the responsibility of each party regarding such actions. | | | |
| **11** | Specify the point at which a party accepts liability for anything that may compromise the personal information while it is in transit to the other party – i.e., is it once the information has reached the servers of the party(ies) receiving the personal information or before or after that point? | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Personal Information Exchange Agreement between the GN and another Government Organization (Federal, Provincial, Territorial, Inuit Organization or Foreign) | | | | |
|---|---|---|---|---|
| | **The Agreement Should…** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **12** | Describe the mechanism by which the two parties will inform the individuals whose personal information is involved in the agreement of the existence of the agreement and its operational requirements. Where the confidential nature of the agreement dictates that its existence should not be revealed to the public, the agreement should contain the rationale for that decision. | | | |
| **13** | Identify any legal provision that may override the terms of the agreement, and what the parties shall do should the existence of any such overriding provision be discovered after the signature of the agreement. | | | |
| **14** | Identify any provision of the other government's privacy law or framework that may be inconsistent with the ATIPP Act, and what the parties shall do should the existence of any such overriding provision be discovered after the signature of the agreement. | | | |
| **15** | Specify that a PIA has been conducted by each party, and in relation to the agreement | | | |
| **16** | Specify that a security TRA has been conducted by both parties (or jointly) in relation to the equipment and the processes that will be used to exchange the information. | | | |
| **17** | Specify the rights of the GN or public body, including the recourse that can be exercised by the GN or public body in case of non-compliance with the terms of the agreement by the other party. | | | |
| **18** | Specify the recourse available to the individuals who wish to challenge any aspect of the agreement. | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Personal Information Exchange Agreement between the GN and another Government Organization (Federal, Provincial, Territorial, Inuit Organization or Foreign) | | | | |
|---|---|---|---|---|
| | **The Agreement Should…** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **Clauses that Pertain to the Personal Information Exchange Activities** | | | | |
| **19** | Specify the nature of the personal information to be exchanged under the agreement. | | | |
| **20** | Identify the categories of individuals whose personal information is covered by the agreement. | | | |
| **21** | Specify the nature of the exchanges – paper based, electronic, etc. | | | |
| **22** | Specify the point of departure and the point of arrival of the information. | | | |
| **23** | Describe the equipment to be used for the exchange. | | | |
| **24** | Specify the conditions (circumstances, system to be used, frequency, etc.) under which the information is to be exchanged. | | | |
| **25** | Specify the frequency of the exchanges. | | | |
| **26** | Describe the uses that can be made of the personal information specified in the agreement by the partiy (ies) receiving the personal information. | | | |
| **27** | Describe the disclosures that can be made of the personal information specified in the agreement by the party (ies) receiving the personal information. | | | |
| **28** | Specify the information management framework applicable to the personal information covered by the agreement. | | | |
| **29** | Specify the retention and disposition schedule that applies to the personal information covered by the agreement. | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Personal Information Exchange Agreement between the GN and another Government Organization (Federal, Provincial, Territorial, Inuit Organization or Foreign) | | | | |
|---|---|---|---|---|
| | **The Agreement Should…** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **30** | Impose an obligation that both parties ensure that the personal information that is used for decision-making is accurate, up-to-date and complete – and includes a mechanism by which the parties inform one another of any problem regarding the information exchanged under the agreement. | | | |
| **31** | Specify that the party or parties receiving the personal information involved in the agreement are to systematically document all uses and disclosures that are made of it. | | | |
| **32** | Specify the mechanisms to be implemented by each party receiving the personal information, to allow the individuals to whom the personal information pertains to exercise their right to request access to, and correction of it. | | | |
| **33** | Specify that the party or parties receiving the personal information are to implement a mechanism by which they can inform all third parties who have been allowed access to the personal information involved in the agreement during the last year of the fact that the individual to whom the personal information pertains has made a request for its correction. | | | |
| **34** | Specify how the personal information is to be disposed of at the end of its life cycle by all the parties. | | | |
| **35** | Specify the security measures to implement in order to prevent unauthorized access to the personal information involved in the agreement. | | | |
| **36** | Specify the security measures to implement in order to prevent unauthorized modification of the personal information involved in the agreement. | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Personal Information Exchange Agreement between the GN and another Government Organization (Federal, Provincial, Territorial, Inuit Organization or Foreign) | | | | |
|---|---|---|---|---|
| | **The Agreement Should…** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **37** | Specify the security measures to implement in order to prevent unauthorized destruction of the personal information involved in the agreement. | | | |
| **38** | Set the conditions for the protection of the confidentiality and the security of the personal information, both during and after its transmission. | | | |
| **39** | Specify any other condition found to be relevant by the parties to the agreement. | | | |

## Annex 4.6 – Privacy Analysis Table 5 – Privacy Analysis of a Collaborative Agreement between the GN and a Private Sector Organization

This table is to be used in conjunction with the table in Annex 4.4 for the analysis of a collaborative agreement between the GN and a private sector organization.

| Privacy Analysis Table 5<br>Privacy Analysis of a Collaborative Agreement<br>between the GN and a Private Sector Organization | | | | |
|---|---|---|---|---|
| | **The Agreement Should...** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **General Terms of the Agreement** | | | | |
| **1** | Specify, in clear terms, the purpose of the agreement. | | | |
| **2** | Clearly identify the parties to the agreement – by their legal names or identifiers. Where the agreement is signed by a component of an organization (directorate, branch, etc.), the name of that component must be specified in the agreement. | | | |
| **3** | Specify the titles of the individuals in each participating organization who are responsible for ensuring compliance with the terms of the agreement. | | | |
| **4** | Clearly identify the legal, regulatory or policy authority that allows or requires the GN or public body to enter into the agreement. | | | |
| **5** | Clearly identify the corporate authority for the other party to enter into the agreement with the GN or public body. | | | |
| **6** | Specify the duration of the agreement, and the amendment procedure. | | | |
| **7** | Specify the process by which the parties can terminate the agreement before the negotiated expiry date. | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Collaborative Agreement<br>between the GN and a Private Sector Organization | | | | |
|---|---|---|---|---|
| | **The Agreement Should...** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **8** | Specify the responsibilities of each party as they relate to the identification of security and privacy breaches, the reporting of such breaches to the other party, the investigation of those breaches and how the situations are to be addressed – i.e., who informs the individuals whose personal information has been compromised, how this is done, etc. | | | |
| **9** | Identify the provincial or territorial jurisdiction whose laws shall prevail in case of a disagreement or conflict pertaining to the agreement. | | | |
| **10** | Protect each party from the consequences of court actions taken against the other one, and specify the responsibility of each party regarding such actions. | | | |
| **11** | Specify the point at which a party accepts liability for anything that may compromise the personal information while it is in transit to the other party – i.e., is it once the information has reached the servers of the party or parties receiving the personal information or before or after that point? | | | |
| **12** | Describe the mechanism by which the two parties will inform the individuals whose personal information is involved in the agreement of the existence of the agreement and of its requirements. | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Collaborative Agreement<br>between the GN and a Private Sector Organization | | | | |
|---|---|---|---|---|
| | **The Agreement Should...** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **13** | Identify any legal provision that may override the terms of the agreement, and what the parties shall do should the existence of any such overriding provision be discovered after the signature of the agreement. | | | |
| **14** | Specify that a PIA has been conducted by both parties (or jointly) in relation to the agreement. | | | |
| **15** | Specify that a security TRA has been conducted by both parties (or jointly) in relation to the equipment and the processes that will be used to exchange the information. | | | |
| **16** | Specify the rights of the GN or public body, including the recourse that can be exercised by the GN or public body, in case of non-compliance with the terms of the agreement by the other party. | | | |
| **17** | Specify the recourse available to the individuals who wish to challenge any aspect of the agreement. | | | |
| **Clauses that Pertain to the Personal Information Exchange Activities** | | | | |
| **18** | Specify the nature of the personal information to be exchanged under the agreement. | | | |
| **19** | Identify the categories of individuals whose personal information is covered by the agreement. | | | |
| **20** | Specify the nature of the exchanges – paper based, electronic, etc. | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Collaborative Agreement<br>between the GN and a Private Sector Organization | | | | |
|---|---|---|---|---|
| | **The Agreement Should...** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **21** | Specify the point of departure and the point of arrival of the information. | | | |
| **22** | Describe the equipment to be used for the exchange. | | | |
| **23** | Specify the conditions under which the information is to be exchanged. | | | |
| **24** | Specify the frequency of the exchanges. | | | |
| **25** | Describe the uses that can be made of the personal information specified in the agreement by the party or parties receiving the personal information. | | | |
| **26** | Describe the disclosures that can be made of the personal information specified in the agreement by the party or parties receiving the personal information. | | | |
| **27** | Specify the information management framework applicable to the personal information covered by the agreement. | | | |
| **28** | Specify the retention and disposition schedule that applies to the personal information covered by the agreement. | | | |
| **29** | Impose an obligation that both parties ensure that the personal information that is used for decision-making is accurate, up-to-date and complete – and includes a mechanism by which the parties inform one another of any problem regarding the information exchanged under the agreement. | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Collaborative Agreement<br>between the GN and a Private Sector Organization | | | | |
|---|---|---|---|---|
| | **The Agreement Should...** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **30** | Specify that the party or parties receiving the personal information are to systematically document all uses and disclosures that are made of it. | | | |
| **31** | Specify the mechanisms to be implemented by each party receiving the personal information to allow the individuals to whom the personal information pertains to exercise their right to request access to, and correction of it. | | | |
| **32** | Specify that the party or parties receiving the personal information are to implement a mechanism by which they can inform all third parties who have been allowed access to the personal information involved in the agreement during the last year) of the fact that the individual to whom the personal information pertains has made a request for its correction. | | | |
| **33** | Specify how the personal information is to be disposed of at the end of its life cycle by the party or parties receiving the personal information. | | | |
| **34** | Specify the security measures to implement in order to prevent unauthorized access to the personal information involved in the agreement. | | | |
| **35** | Specify the security measures to implement in order to prevent unauthorized modification of the personal information involved in the agreement. | | | |

| Privacy Analysis Table 5<br>Privacy Analysis of a Collaborative Agreement<br>between the GN and a Private Sector Organization | | | | |
|---|---|---|---|---|
| | **The Agreement Should...** | **Agreement Meets the Criteria** | **Agreement Does not Meet the Criteria** | **Observations** |
| **36** | Specify the security measures to implement in order to prevent unauthorized destruction of the personal information involved in the agreement. | | | |
| **37** | Set the conditions for the protection of the confidentiality and the security of the personal information, both during and after its transmission. | | | |
| **38** | Specify any other condition found to be relevant to the circumstances of the agreement. | | | |

# Annex 4.7 – Privacy Analysis Table 7 – Analysis of External Party Privacy Policy before the Signing of an Information Sharing Agreement

This table is to be used in conjunction with the tables in Annex 4.4 and, where applicable, with Annex 5 or 6 for the analysis of the privacy policy of an organization with which the GN is considering signing an information sharing agreement.

| Privacy Analysis Table 7<br>Analysis of External Party Privacy Policy before<br>the Signing of an Information Sharing Agreement | | | | |
|---|---|---|---|---|
| | **Criteria** | **Policy Meets the Criteria** | **Policy Does not Meet the Criteria** | **Observations** |
| **General Terms of the Policy** | | | | |
| **1** | The policy clearly identifies the organization (or the unit within) that has issued the policy. | | | |
| **2** | The policy specifies its purpose in clear terms. | | | |
| **3** | The policy clearly identifies the privacy legislation that applies to the organization. | | | |
| **4** | The policy clearly identifies any other organization to which it may also apply. | | | |
| **5** | The policy specifies the date of its coming into effect and/or the last date of amendment. | | | |
| **6** | The policy clearly identifies the legal provisions that may override the terms of the policy, such as mandatory reporting legislation that may apply to certain types of activities, etc. | | | |
| **7** | The policy is easily available to the clients and employees of the organization. | | | |

| Privacy Analysis Table 7<br>Analysis of External Party Privacy Policy before<br>the Signing of an Information Sharing Agreement | | | | |
|---|---|---|---|---|
| **8** | The policy is presented to the individual at the very beginning of a transaction or other significant interaction that involves the exchange of personal information about the individual. | | | |
| **Collection of personal information** | | | | |
| **9** | The policy describes clearly the elements of personal information that are collected by the organization. | | | |
| **10** | The policy specifies the circumstances under which the organization collects personal information. | | | |
| **11** | The policy specifies whether or not the individuals who interact with the organization are obligated to provide their personal information. | | | |
| **12** | The policy describes the means by which it collects personal information – i.e., direct or indirect collection, in person, via its website, etc. | | | |
| **13** | The policy provides advice or guidance to individuals on the security and privacy risks that they incur when they use certain unsafe means to share their personal information with the organization – i.e., by email, fax, etc. | | | |
| **14** | The policy provides the name or title, address and/or telephone number of an employee who can answer questions about the collection of the personal information. | | | |

| Privacy Analysis Table 7<br>Analysis of External Party Privacy Policy before<br>the Signing of an Information Sharing Agreement | | | | |
|---|---|---|---|---|
| **15** | The policy refers to the "cookies" and other electronic means that the organization uses to monitor how they use the organization's website. | | | |
| **16** | The policy explains what the organization will do with the personal information that its servers collect about the visitors of its website. | | | |
| **17** | Where applicable, the policy explains that by clicking on certain links the visitors may be taken to the website of another organization and that they are advised to read the privacy policy of that other organization before engaging in activities that may pose privacy or other risks. | | | |
| **Consent of the individual who is the subject of the personal information.** | | | | |
| **18** | The policy states that consent will be sought from the individual before his or her personal information is collected, used or disclosed by the organization. | | | |
| **19** | The policy explains the consequences that may result if the individual gives consent. | | | |
| **20** | The policy explains the consequences that may result if the individual refuses to give consent. | | | |
| **21** | The policy offers individuals the choice of "opting-out" in regard to the collection, use and disclosure of their personal information. | | | |
| | | | | |

| Privacy Analysis Table 7<br>Analysis of External Party Privacy Policy before<br>the Signing of an Information Sharing Agreement | | | | |
|---|---|---|---|---|
| **Use of personal information.** | | | | |
| **22** | The policy describes all the uses that the organization makes of the personal information under its control. | | | |
| **23** | The uses that the organization makes of the personal information under its control are all legitimate and consistent with the organization's mission, legislative mandate (where applicable). The uses are all of a type that most individuals would consider "reasonable". | | | |
| **Disclosure of personal information.** | | | | |
| **24** | The policy describes all the disclosures that the organization makes of the personal information under its control. | | | |
| **25** | The disclosures that the organization makes of the personal information under its control are all legitimate and consistent with the organization's mission, legislative mandate (where applicable). The uses are all of a type that most individuals would consider "reasonable". | | | |
| **26** | The organization limits the disclosure of personal information to those circumstances where it is required or authorized to do so by law, and in those circumstances it discloses only the elements of personal information that need to be disclosed. | | | |
| | | | | |

| Privacy Analysis Table 7<br>Analysis of External Party Privacy Policy before the Signing of an Information Sharing Agreement | | | | |
|---|---|---|---|---|
| **Retention of personal information.** | | | | |
| **27** | The policy specifies the retention period that applies to the personal information under the organization's control. | | | |
| **28** | The policy specifies whether or not an individual can ask to have his or her personal information destroyed or deleted before the end of the established retention schedule. | | | |
| **29** | The policy explains whether or not an individual can ask that the personal information be retained by the organization after the end of the established retention schedule. | | | |
| **Disposition of the personal information.** | | | | |
| **30** | The policy specifies how the personal information under the organization's control is disposed of at the end of its life cycle. | | | |
| **Accuracy of the personal information.** | | | | |
| **31** | The policy explains the measures taken by the organization to ensure that the personal information that it uses to make decisions about individuals is as accurate, up-to-date and complete as possible. | | | |
| **32** | The policy explains the measures taken by the organization to ensure that the personal information that it shares with other parties is as accurate, up-to-date and complete as possible. | | | |
| | | | | |

| Privacy Analysis Table 7<br>Analysis of External Party Privacy Policy before<br>the Signing of an Information Sharing Agreement | | | | |
|---|---|---|---|---|
| **Safeguarding (protection) of the personal information.** | | | | |
| **33** | The policy explains how the organization generally tries to ensure the protection of the personal information under its control against unauthorized access, use, modification and destruction. | | | |
| **Right of the individual to request access to his or her own personal information.** | | | | |
| **34** | The policy explains how individuals can request access to their own personal information which is kept by the organization. | | | |
| **Right of the individual to request the correction of his or her personal information.** | | | | |
| **35** | The policy explains how individuals can request the correction of their own personal information which is kept by the organization. | | | |
| **Recourse when the organization is alleged to not comply with the applicable privacy legislation.** | | | | |
| **36** | The policy specifies the recourse available to the individuals who wish to challenge any aspect of the policy. | | | |

# Annex 4.8 – Privacy Analysis Table 8 – Retention and Disposition

| Privacy Analysis Table 8<br>Retention and Disposition | | | |
|---|---|---|---|
| | **Criteria** | **Assessment** | **Observations** |
| **1** | Retention schedule for the personal information that is involved in the initiative. | | |
| **2** | Legal, regulatory or policy authority for the retention – Records Disposition Authority 1995-32. | | |
| **3** | Specify if the individuals to whom the personal information pertains have been adequately informed of the retention schedule. | | |
| **4** | Describe the method/means that will be used to retain the information. | | |
| **5** | Describe the measures in place to ensure that all the copies of the information are disposed of at the end of the approved retention schedule. | | |
| **6** | Describe the measures in place to easily retrieve the personal information in case the individual to whom it pertains would request that it be destroyed before the end of its approved retention period. | | |
| **7** | Risks associated with the retention – the fact that the information is being retained, the environmental and electronic conditions of the retention, risks for the parties responsible for its retention and individuals to whom the personal information pertains, possibility of a legal challenge or embarrassment for the GN or public body, etc. | | |
| This form last revised: May, 2013 | | | |

# Annex 4.9 – Privacy Analysis Table 9 – Accuracy and Integrity

| Privacy Analysis Table 9<br>Accuracy and Integrity | | | |
|---|---|---|---|
| | **Criteria** | **Assessment** | **Observations** |
| **1** | Mechanisms that are in place to ensure that the personal information that is involved in the initiative is accurate, complete and up-to-date (all copies in any format). | | |
| **2** | Mechanisms that are in place to detect errors and integrity issues. | | |
| This form last revised: January 2013 | | | |

# Annex 4.10 – Privacy Analysis Table 10 – Safeguarding

| Privacy Analysis Table 10<br>Safeguarding – Administrative, Physical and Technical Aspects | | | |
|---|---|---|---|
| | **Criteria** | **Assessment** | **Observations** |
| **1** | Security procedures for the collection, transmission, storage and disposition of personal information, and access to it. | | |
| **2** | Security measures / controls in place for the initiative, including:<br>• configuration and characteristics of the systems used for the collection of personal information;<br>• regular audits, inspections and verifications;<br>• investigations into breaches;<br>• safeguards to prevent the unauthorized modification of the personal information. | | |
| **3** | List the weaknesses and recommendations contained in the security TRA report and management's responses to the recommendations. | | |
| **4** | Interruption in the delivery of the programs or services of the organization should a security incident affect the personal information. | | |
| **5** | Risk to the safety of individuals should a security incident affect the personal information. | | |
| **6** | Financial fraud or theft should a security incident affect the personal information. | | |
| **7** | Commission of other types of criminal acts should a security incident affect the personal information. | | |
| **8** | Difficulty for the GN or public body to negotiate information sharing agreements with other organizations or termination of such agreements should a security incident affect the personal information. | | |

| Privacy Analysis Table 10<br>Safeguarding – Administrative, Physical and Technical Aspects | | | |
|---|---|---|---|
| **9** | Consequences for the GN or public body should a security incident affect the personal information. | | |
| **10** | Temporary or permanent loss of critical or valuable information should a security incident affect the personal information. | | |
| **11** | Loss, destruction or theft of valuable or critical assets should a security incident affect the personal information. | | |
| | This form last revised: May 2013 | | |

# Annex 4.11 – Privacy Analysis Table 11 – Individuals' Access and Correction Rights

| Privacy Analysis Table 11<br>Individuals' Access and Correction Rights | | | |
|---|---|---|---|
| | **Criteria** | **Assessment** | **Observations** |
| **1** | Description of the measures in place to facilitate the exercise of the individuals' right to request access to, and the correction of the personal information that is involved in the initiative. | | |
| This form last revised: May 2013 | | | |

# Appendix 5 – Privacy Impact Assessment – Summary of PIA Findings

| Summary of PIA Findings | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Categories of Individuals** | **Elements of Personal Information** | **Collection Source, Method and Consent** | **Purpose of Collection** | **Collection Method** | **Storage Format** | **Uses** | **Disclosures** | **Retention and Disposition Schedule** |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| This form last revised: May 2013 | | | | | | | | |

## Appendix 6 – Privacy Impact Assessment – Proposed Schedule for the Implementation of the Recommendations

| Proposed Schedule for the Implementation of the Recommendations | | | |
|---|---|---|---|
| | **Weaknesses Identified** | **Suggestions / Recommendations** | **Suggested Time Frames for the Implementation of the Recommendations** |
| **1** | | | |
| **2** | | | |
| **3** | | | |
| **4** | | | |
| **5** | | | |
| **6** | | | |
| **7** | | | |
| **8** | | | |
| This form last revised: May 2013 | | | |

# Section 8:

# Procedure for the Conduct of Privacy Inspections and Privacy Compliance Audits

## Table of Contents

# 1. Introduction

This manual supports the GN's Privacy Program by describing the concepts and the step-by-step approach for the conduct of privacy inspections and privacy compliance audits. It is designed to assist the ATIPP manager and the ATIPP coordinators for public bodies in their efforts to prevent privacy incidents and privacy breaches by identifying existing gaps and weaknesses in the systems, policies and practices of public bodies.

# 2. Objectives

As a way to ensure that the GN programs, services and activities are conducted in compliance with the requirements of Part 2 of the *ATIPP Act* and the generally accepted privacy principles, these procedures aim to ensure that:

8.3 existing gaps and weaknesses in the systems, policies and practices of public bodies are promptly identified through the regular conduct of privacy inspections and privacy compliance audits;

8.4 the terms of all existing and potential partnering and stakeholder relationships and agreements are complied with by all parties;

8.5 program directors can better plan the development and the implementation of measures to protect the personal information under their control, as well as save on costs;

8.6 public bodies can demonstrate that they fulfill their obligations as they relate to the implementation of measures aimed at preventing privacy incidents and privacy breaches.

# 3. Definitions

**Gap:** in relation to privacy protection, refers to the absence of adequate norms, standards or instructions to guide employees in their day-to-day activities. It may result in employees not handling the personal information of clients or other employees in compliance with the requirements of the *ATIPP Act* and the generally accepted principles.

**Privacy Compliance Audit:** is a comprehensive review process that is typically conducted for an entire program, service or a large and important activity of a public body. It is similar to a privacy impact assessment (PIA) in that:

- it is based on the same legal and technical criteria;
- it involves a thorough examination of the relevant policies, systems and practices to identify areas of non-compliance and vulnerabilities;

- it may lead to the formulation of recommendations to enhance the privacy compliance of the program, service or activity.

Where the audit uncovers evidence of serious errors, flaws in the administration of a program or evidence of malicious acts, a recommendation will be made that a detailed investigation be conducted. Because of their encompassing nature, privacy compliance audits are more demanding in terms of time and resources than privacy inspections.

**Privacy Inspection:** aims to verify the compliance of a particular aspect of a program, service, agreement or activity with the requirements of the *ATIPP Act* and the generally accepted privacy principles. Because it focuses on a very specific aspect, its scope is fairly narrow and it requires fewer resources than a full-scale privacy compliance audit. A privacy inspection may take from a few minutes to a few hours to conduct and, depending upon the circumstances, it may lead to a recommendation that a full-scale audit or investigation be conducted.

**Weakness:** in relation to privacy protection, refers to the absence of adequate security measures to protect the personal information which is under the control of a public body. Weaknesses include (but are not limited to):

- the absence of, or the existence of inadequate firewall or antivirus applications in a public body's electronic information management or communications system;
- a weak user identification mechanism to access a public body's electronic information management or communications system;
- a lack of proper monitoring mechanism of a public body's electronic information management or communications system;
- the absence of adequate post-audit features in a public body's electronic information management or communications system;
- the absence of adequate physical security controls in a facility where personal information is stored or processed.

# 4. Conducting Privacy Inspections and Privacy Compliance Audits

## *4.1 Considerations when Planning to Conduct a Privacy Inspection or a Privacy Compliance Audit*

4.1.1 The characteristics of the facility, program, service, activity or system to be inspected or audited;

4.1.2 The importance of the program, service, activity or system for clients and GN employees;

4.1.3 The sensitivity of the personal information that is collected, used or kept by the program, service or activity;

4.1.4 The threat and risk factors that are specific to the program, service, activity or system;

4.1.5 The history of privacy incidents and privacy breaches in respect to the program, service, activity or system;

4.1.6 The ideal scope of the inspection or audit, considering the circumstances;

4.1.7 The resources required for the conduct of the inspection or audit – required skills and number of individuals involved;

4.1.8 Any other relevant factor.

## *4.2 When to Conduct Privacy Inspections and Privacy Compliance Audits*

4.2.1 Every year for those areas that have been identified to present the highest potential for privacy invasion and privacy breaches (the privacy analysis tables in the PIA procedure manual may be used for that analysis);

4.2.2 Following a program modification that may potentially have adverse consequences on the privacy of individuals;

4.2.3 In all other circumstances where, in the opinion of the DM, ADM, a director or ATIPP coordinator of a public body, an inspection or an audit should be conducted.

## *4.3 Requirements for Conducting Privacy Inspections and Privacy Compliance Audits*

4.3.1 The ATIPP coordinators are responsible for compiling statistics on the number of inspections and audits conducted during each fiscal year and report those figures to the ATIPP manager, EIA;

4.3.2 Inspections and audits must be conducted in a manner that respects the rights and the dignity of the employees. They must also be conducted in a manner that minimizes their negative impact on operations;

4.3.3 As the DM is the delegated head of the public body, his/her approval should be sought prior to an inspection or audit. The ADM and director or manager responsible for the service or program to be inspected or audited should be informed before the beginning of the inspection or the audit. They should be told exactly what will happen, when it will happen and what the next steps are.No notice shall be given when doing so may jeopardize the integrity of the inspection or the audit.

4.3.4 The ATIPP coordinator must document all evidence of serious errors, flaws in the practices, malicious acts that are uncovered during the inspection or the audit;

4.3.5 The ATIPP coordinator must transfer to the DM, ADM, director or manager responsible for the service or program all evidence of serious errors, flaws in the practices and malicious acts;

4.3.6 Where applicable, the ATIPP coordinator must report the serious anomalies uncovered during the inspection or audit to the ATIPP manager at EIA. EIA will decide on a case by case basis whether the anomalies should be reported to the Information and Privacy Commissioner and, where appropriate, the parties who have an interest in the information (e.g., the partners of the information sharing agreement, the RCMP or other authority);

4.3.7 The ATIPP coordinator must inform all interested parties of the results of the inspections and audits, along with the recommendations that may affect them.

## *4.4 Systematic Approach in Conducting Privacy Inspections and Privacy Compliance Audits*

A systematic approach for the conduct of privacy inspections and privacy compliance audits ensures that:

4.4.1 all of the parties involved understand their respective roles and responsibilities and contribute positively to the process;

4.4.2 the rights of all of the parties involved in the process are respected at all times, in accordance with the due process principle, the applicable legal and policy requirements and the principle of fairness;

4.4.3 all relevant aspects are properly examined and documented, in accordance with the inspection or audit plan;

4.4.4 the conduct and the results of all inspections and audits are presented in a consistent manner;

4.4.5 the conclusions are based on demonstrable evidence and adequately supported by facts;

4.4.6 the decisions that result from the conduct of a privacy inspection or privacy compliance audit are properly documented.

## *4.5 Privacy Inspection and Privacy Compliance Audit Process*

### 4.5.1 Inspection or Audit Plan:

As a way to ensure an orderly process, a plan detailing the following aspects must be prepared before the beginning of every privacy inspection and audit:

4.5.1.1 the reason and the purpose of the inspection – what triggered it;

4.5.1.2 the purpose of the audit and what motivated the selection of the specific program, service, activity or system for inspection or audit;

4.5.1.3 the scope of the inspection or audit;

4.5.1.4 the criteria that will serve as a basis for the assessment;

4.5.1.5 the inspection or audit process to be followed;

4.5.1.6 the information sources – documentation, interviews with employees, contractors, clients, etc. – from which the information will be obtained;

4.5.1.7 the resources required for the inspection or the audit – including the number of individuals required and their qualifications;

4.5.1.8 the time frame set for the completion of the inspection or the audit;

4.5.1.9 any other relevant aspect.

### 4.5.2 Informing the Interested Parties:

Under normal circumstances, a written notice will be sent to the interested parties ahead of the beginning of the inspection or the audit. The notice may include a statement specifying that they will be met by the individuals responsible for the inspection or audit and, where applicable, that they gather all the relevant information prior to the interview.

No such notice shall be sent where it is feared that informing the parties ahead of time may jeopardize the integrity of the inspection or audit.

### 4.5.3 Information Collection:

Information may be collected from any source, in accordance with the applicable laws, regulations, policies and contractual agreements. The information shall not be collected by covert means, except where openly collecting it would risk jeopardizing the integrity of the inspection or audit process. The ATIPP manager, EIA, must be consulted before any covert means are used for the collection of information, and a legal opinion on the legal validity of the considered approach may have to be obtained.

### 4.5.4 Analysis and Conclusions:

The results of the inspection or audit shall be discussed with the interested parties before the report is produced so that these parties can respond adequately and, where appropriate, have their views incorporated into the report.

### 4.5.5 Report:

The ATIPP coordinator shall submit all inspection and audit reports to the ATIPP manager, EIA, to determine the best course of action to take with respect to the issues that were identified during the assessment process.

## Appendix 1 – Recommended Qualifications of External Resources for the Conduct of Privacy Compliance Audits

The following criteria aim to ensure that external resources (contractors) granted a contract to conduct privacy compliance audits for the GN are properly qualified and that they possess a solid understanding of the mandate, operation and culture of the GN.

1. **Education and Privacy Work Experience:**

   a) A university degree in the arts, social sciences, law or public / business administration from a recognized university, **and** at least four years of continued experience in the privacy protection field within the last five years;

   **OR**

   b) High school diploma (or a General Equivalency Diploma), and at least five years of continued experience in the privacy protection field within the last six years.

2. **Formal Privacy Training:**

   Three days or more of formal privacy training by a credible / reputed organization should be considered an asset qualification.

3. **Experience in the Conduct of PIAs, Privacy Compliance Audits or Privacy Breach Investigations:**

   Experience acquired through the conduct of a combined total of at least ten (10) PIAs and / or privacy compliance audits and / or privacy breach investigations during the last three years.

4. **Experience in the Analysis or the Development of Privacy Frameworks for Government Institutions:**

   a) Three years of experience in developing detailed, documented analyses of any Canadian jurisdiction's privacy framework, especially the GN *ATIPP Act*;

   **OR**

   b) Three years' experience in the development of privacy frameworks for a Canadian jurisdiction.

**5. Knowledge of the Mandate, Operation and Organizational Culture of the GN:**

All candidates shall demonstrate a deep understanding of the mandate, operation and organizational culture of the GN.

**6. Privacy Experience in Other Canadian Jurisdictions:**

A wide range of experience in the privacy protection field with the provincial, territorial or municipal public sector or with First Nations governments, where that experience is consistent with the mandate, operation and culture of the GN, should be considered an asset qualification.

**7. Experience in the Security Field:**

An in-depth knowledge of the security principles **and** who have conducted numerous security threat and risk assessments (TRA) for a Canadian jurisdiction should be should be considered an asset qualification, provided that candidates demonstrate a full understanding of the differences between:

a) security and privacy;

**AND**

b) the PIA and the TRA processes.

**8. Experience in the Conduct of Investigations:**

The candidates must possess a combination of formal class training and at least four years of experience in the conduct of investigations in the security, human rights or human resources fields. Knowledge of the criminal investigation process would be an asset qualification.

## Appendix 2 – Forms and Templates

The following tables have been included as operational aids to facilitate resolution of a privacy breach.

## Appendix 2.1 – Statistical Report on Privacy Inspections and Privacy Compliance Audits for Fiscal Year: (insert year)

The table below is to be used by ATIPP coordinators to document the statistical figures pertaining to the results of the privacy inspections and privacy audits conducted during the fiscal year.

| | Identification of Program, Unit, Service, System, etc. | Inspected or Audited |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |
| 7 | | |
| 8 | | |
| 9 | | |
| 10 | | |
| 11 | | |

## Appendix 2.2 – Privacy Inspection / Privacy Compliance Audit Report

| Status as a Privacy Inspection or Privacy Compliance Audit Report<br>(Please provide rationale and append all the relevant documentation to this report.) | | |
|---|---|---|
| 1 | Date of the report. | |
| 2 | Author(s) of the report. | |
| 3 | Contact information for the author(s) of the report. | |

| Status as a Privacy Inspection or Privacy Compliance Audit Report<br>(Please provide rationale and append all the relevant documentation to this report) | | |
|---|---|---|
| 5 | Privacy Inspection | Privacy Compliance Audit |
| 6 | | |

| Nature of the Gaps and Weaknesses Identified<br>(for statistical purposes) | | |
|---|---|---|
| 7 | ☐ Risks associated with the collection of personal information<br>☐ Risks associated with the use of personal information<br>☐ Risks associated with the modification of personal information<br>☐ Risks associated with the accuracy of personal information<br>☐ Risks associated with the disclosure of personal information<br>☐ Risks associated with the retention of personal information<br>☐ Risks associated with the destruction of personal information | ☐ Risks associated with the access to information management or communications systems<br>☐ Risks associated with the loss of personal information or asset that contained personal information<br>☐ Risks associated with the misfiling of personal information<br>☐ Other risks uncovered – please specify: |

| Details of the Gaps and Weaknesses Identified | | | |
|---|---|---|---|
| | **Reporting Criteria** | **Findings** | **Recommendations** |
| **8** | Gaps or weaknesses associated with the collection of personal information. | | |
| **9** | Gaps or weaknesses associated with the use of personal information. | | |
| **10** | Gaps or weaknesses associated with the modification of personal information. | | |
| **11** | Gaps or weaknesses associated with the accuracy of personal information. | | |
| **12** | Gaps or weaknesses associated with the disclosure of personal information. | | |
| **13** | Gaps or weaknesses associated with the retention of personal information. | | |
| **14** | Gaps or weaknesses associated with the destruction of personal information. | | |
| **15** | Gaps or weaknesses associated with the access to information management or communications systems. | | |
| **16** | Gaps or weaknesses associated with the loss of personal information or asset that contained personal information. | | |
| **17** | Gaps or weaknesses associated with the misfiling of personal information. | | |
| **18** | Other gaps or weaknesses uncovered – please specify: | | |

| Parties Who Can Provide Information about the Gaps or Weaknesses | | |
|---|---|---|
| | **Names** | **Titles and Coordinates** |
| **19** | | |
| **20** | | |
| **21** | | |
| **22** | | |

| Narrative Section | |
|---|---|
| **23** | **Introduction** |
| **24** | **Brief Description of the Program, Unit, Service, System, etc. that Was the Subject of the Inspection or Audit** |
| **25** | **What Prompted the Inspection or Audit** |
| **26** | **Approach and Methodology for the Conduct of the Inspection or Audit** |
| **27** | **Findings** |
| **28** | **Conclusion(s)** |
| **29** | **Recommendations** |
| **Signature Block** | |
| **30** | _____<br>Signature of ATIPP coordinator |

This form last revised May, 2013

## Report Appendix 1 – Summary of Inspection or Audit Activities

| | Activities | Dates | Observations |
|---|---|---|---|
| **1** | Beginning of the audit: | | |
| **2** | •Preliminary gathering of information<br>•Preparation of audit plan<br>•Drafting of letters to invite witnesses to interviews<br>•Preliminary identification of witnesses | | |
| **3** | Appointments scheduled and convocation letters sent to the witnesses | | |
| **4** | Interviews with witnesses | | |
| **5** | Other activities | | |
| **6** | Submission of interim report | | |
| **7** | Comments received from the interested parties | | |
| **8** | Writing of final audit report | | |
| **9** | Submission of final audit report | | |

## Report Appendix 2 – Example of an Audit Plan

| Activity | Date | Comments |
|---|---|---|
| Beginning of the audit: | | This is the date on which the audit mandate is approved. |
| • Preliminary gathering of information<br>• Preparation of audit plan<br>• Drafting of letters to invite witnesses to interviews<br>• Preliminary identification of witnesses | | |
| Appointments scheduled and convocation letters sent to the witnesses. | | |
| Interviews with witnesses. | | As per accompanying list of interviewees. |
| Submission of preliminary inspection or audit report. | | |
| Comments received from department on the preliminary inspection or audit report. | | |
| Writing of final inspection or audit report. | | |
| Submission of final inspection or audit report. | | |

## Report Appendix 3 – Contributors to the Inspection or Audit Process

| | Names | Titles and Coordinates |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

## Report Appendix 4 – Interviewees

| | Names | Titles and Coordinates |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |

## Report Appendix 5 – Witness Statements and Interview Notes

**Name of interviewee:**

**Status of interviewee:**
(Employee, contractor, client, etc.)

**Title:**
(For employees)

**Place of work:**
(For employees and contractors)

**Date of interview:**

**Time of interview:**

**Place of interview:**

**Purpose of nterview:**

**Summary of interview:**

Report facts and other information as provided by the witness – from the interview notes

## Report Appendix 6 – Inspector / Auditor's Notes and other Documentary Evidence

| | Description of Appended Document or Description and Location of Other Type of Object Used as Evidence |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |

## Report Appendix 7 – Other Relevant Documents

| | Description of Appended Document |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |