



## EXECUTIVE AND INTERGOVERNMENTAL AFFAIRS

### PRIVACY BREACH AND INCIDENT POLICY

---

#### **POLICY STATEMENT**

The Government of Nunavut (GN) recognizes the need to ensure the personal information of individuals is securely protected against unlawful collection, use, disclosure and disposal. This policy sets out requirements of all public bodies to ensure a consistent and standardized approach to preventing and responding effectively to privacy breaches and privacy incidents.

#### **PRINCIPLES**

This policy supports Pijitsirniq and Piliriqatigiinni<sup>q</sup> by ensuring that:

- Public bodies have a duty to ensure the privacy rights of all individuals who provide their personal information to the government; and
- A consistent approach to the application of the privacy provisions of the Act and regulations must be applied across all public bodies.

#### **APPLICATION**

This policy applies to all departments, branches and offices of the Government of Nunavut, as well as agencies, boards, commissions, corporations, offices and other bodies designated under Schedule A of the Access to Information and Protection of Privacy (ATIPP) Regulations except where a public body has developed an internal policy that the Minister responsible for the *Access to Information and Protection of Privacy Act* deems to be substantially similar to this policy.

It also applies to stakeholders, partners, contractors and other representatives of the GN involved in the collection and handling of personal information or information that may have an impact upon individuals' privacy.

#### **DEFINITIONS**

Act:

*The Access to Information and Protection of Privacy Act.*

ATIPP Coordinator:

A public servant with appropriate training and delegated authority to process requests made under the ATIPP Act.

ATIPP Coordinators Committee:

A committee comprised of all ATIPP coordinators of every public body authorized under Section 69 of the ATIPP Act, which is chaired by the Manager of the Territorial ATIPP Office.

Public Body:

A department, branch or office of the Government of Nunavut, or an agency, board, commission, corporation, office or other body designated under Schedule A of the ATIPP Regulations; public bodies do not include the Office of the Legislative Assembly, the office of a member of the Legislative Assembly or Executive Council.

Head:

The member of the Executive Council who presides over a public body that is a department, branch or office of the Government of Nunavut, and in relation to any other public body, the person designated in the regulations as the head of the public body.

Information Technology Division:

The information and technology divisions within the Department of Community and Government Services or any other technical branch that provides support services to a public body.

Deputy Head:

In relation to a department, the Deputy Minister of that department, and in relation to any other portion of the public service, the chief executive officer of that portion or, if there is no chief executive officer, such person as the Minister responsible for the *Public Service Act* may designate as deputy head.

Territorial ATIPP Office:

The office within the Department of Executive and Intergovernmental Affairs designated as the centralized office for the coordination of the ATIPP function across all public bodies.

Privacy Breach:

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 that could result in information being accessed or disclosed without authority. Breaches can be intentional or unintentional and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

Privacy Incident:

A privacy incident is typically less severe than a privacy breach. An incident occurs when personal information is mishandled or incorrectly collected, used or

disclosed. However, unlike a privacy breach, the situation can be corrected easily and quickly without any prejudice to the individual.

Incidents are usually resolved immediately by the employees who become aware of them. Repeated privacy incidents can escalate into a full-scale breach if they are not addressed. Examples of privacy incidents include inadvertent storage of personal information that can be resolved immediately by properly filing the misfiled record; or the temporary unavailability of personal information that is necessary for a decision making process, thus causing a delay in that decision making process; or an input error of personal information that is corrected before any final decision is made about the individual. Minor incorrect collections, uses or disclosures of personal information can be addressed by immediately ceasing the activity and taking steps to ensure it does not happen again.

#### Privacy Impact Assessment (PIA):

The Privacy Impact Assessment (PIA) process is a risk management tool 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 Act.

#### Privacy Management Manual (PMM):

Comprehensive set of instructional materials that outline the standard processes that should be followed by all public bodies in preventing, responding to and addressing privacy incidents and breaches. The PMM is to be maintained and reviewed regularly by the ATIPP office and the ATIPP Coordinators Committee.

## **ROLES AND RESPONSIBILITIES**

### Minister

The Minister responsible for the Act is accountable to the Executive Council for the implementation of this policy.

### Deputy Minister

The Deputy Minister of the Department of Executive and Intergovernmental Affairs is responsible to the Minister for the administration of this policy.

## **PROVISIONS**

All employees are required to comply with the privacy provisions set out in the ATIPP Act and regulations. Privacy breaches may bring serious consequences for the individual and/or the public body, and they may require immediate and comprehensive measures to minimize the damage.

To support the Act and regulations, the PMM will provide the tools needed to allow for the easy implementation of a standard privacy function that is consistent across all public bodies. For a detailed description of the measures and forms

required to respond to and prevent privacy incidents and breaches, please consult the PMM.

**Responding to Privacy Incidents:**

Privacy incidents do not require the conduct of a full-scale investigation. However, employees must take immediate corrective action to resolve the incident to prevent any adverse consequence for the individual as well as for the public body. Appropriate actions to respond to incidents would involve 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.

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

**Responding to Privacy Breaches:**

All public bodies are responsible for responding to privacy breaches in accordance with predetermined processes. These are as follows:

**Stop the Breach:** Immediate action must be taken to prevent a further invasion of the privacy of all the individuals who are affected by the breach.

**Limit the Harm:** Action must be taken to minimize the gravity of the consequences for the individuals who are affected by the breach.

**Document the Circumstances:** The circumstances of the breach must be fully documented.

**Investigate:** The ATIPP Coordinator within the public body will oversee the investigative process and report all findings to their Deputy Head and 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 as well as 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 (in the case of the GN, the

Department of Justice) and the Risk Management Division of the Department of Finance.

**Notify the Individual(s) Affected by the Breach:** 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. 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 protect themselves adequately.

**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) of the Act.

**Take other Appropriate Actions as Directed by the Circumstances:** Pending on the nature of the privacy breach, further actions may be required, such as issuing a press release, or contacting police forces. Further Actions will be determined by the ATIPP Manager in consultation with the Deputy Head, legal counsel, Risk Management and any other relevant authorities. Corrective and preventative measures suggested or recommended by the Information and Privacy Commissioner will be given proper consideration.

**Prevention of Privacy Breach or Incident:**

To prevent privacy breaches or incidents from occurring, project leads will be required to complete project initiation summaries for any new, or amendments to an existing, project or system that consists of the collection, storage or use of personal information. This summary will be reviewed by both the ATIPP Coordinator and the ATIPP Manager and used to determine the need for a privacy impact assessment (PIA). Even if the initial review does not identify the need for a PIA, the need for a PIA may be identified later.

**ATIPP Coordinators Committee and Territorial ATIPP Office:**

The ATIPP Coordinators Committee is responsible for developing and reviewing procedures, protocols, guidelines, resource materials and standards of application and service pertaining to the administration of the privacy provisions of the ATIPP Act and its regulations.

The Territorial ATIPP Office will:

- 1) Monitor the implementation of this policy and related procedures to ensure that all public bodies implement adequate measures to prevent and respond to privacy breaches and privacy incidents;
- 2) Compile statistical information pertaining to privacy breaches;
- 3) Centrally coordinate response measures for serious privacy breaches; and
- 4) Ensure the accuracy of the PMM and its application across all public bodies.

### **PREROGATIVE OF CABINET**

Nothing in this policy shall in any way be construed to limit the prerogative of the Executive Council to make decisions or take actions respecting the administration of ATIPP outside the provisions of this policy.

### **SUNSET CLAUSE**

This policy will be effective from the date of signature until May 1, 2018.