



## Protection of Privacy Policy

### 1. Statement of Policy

The Government of the Northwest Territories (GNWT) is committed to protecting personal information collected and held by government and recognizes that this protection is critical to maintaining public trust, is an essential element of good governance and needs to be applied and administered by the Government consistently and fairly.

### 2. Principles

The GNWT will adhere to the following principles when applying this Policy:

- (1) The Public should be confident that the GNWT will consistently and fairly protect the information entrusted to them.
- (2) The protection of privacy should be the responsibility of each GNWT department.
- (3) Protection of privacy should be considered as part of the development and delivery of all government programs and services.
- (4) Protection of privacy should be incorporated into the regular activities of all GNWT employees.

### 3. Scope

This Policy applies to departments of the GNWT and the Northwest Territories Housing Corporation (NWT HC) and their employees. Other Public Bodies under the Act may elect to adopt the Protection of Privacy Policy for their employees, but are not bound by it.

The *Access to Information and Protection of Privacy Act* is the legislative authority for the Government of the Northwest Territories to act on privacy matters.

The protection of personal health information as set out in the *Health Information Act* is not part of the GNWT Protection of Privacy Policy. Protection of personal health information is the responsibility of health information custodians who are primarily outside of the scope of this policy. For more information on protection of health

information please contact the Chief Health Privacy Officer at the Department of Health and Social Services.

#### **4. Definitions**

The following terms apply to this Policy:

**Deputy Heads** – The deputy minister of a department, the chief executive officer of a public committee, board or council or such person as may be appointed as deputy head.

**Personal Information** - Means information about an identifiable individual as defined in the *Access to Information and Protection of Privacy Act* (the Act).

**Departmental Privacy Officer** - Is the senior management individual designated by a Deputy Head to be responsible for privacy and the implementation of this Policy and the departmental privacy management program.

**Privacy Breach** – “Privacy Breach” is an unauthorized access, collection, use, or disclosure of personal information, whether accidental or deliberate, that is not authorized by the Act.

**Privacy Impact Assessment** - Is the principal tool used in Canada to ensure that programs and information technology systems and applications are compliant with the jurisdictions’ privacy laws.

**Personal Information Sharing Agreement** – Is an agreement between a GNWT department and either another GNWT public body, or federal government department that sets the conditions regarding the collection, use and/or disclosure of personal information.

#### **5. Authority and Accountability**

##### **(1) General**

This Policy is issued under the authority of the Executive Council. The authority to make exceptions and approve revisions to this Policy rests with the Executive Council. Authority and accountability is further defined as follows:

##### **(a) Ministers**

Ministers are accountable for the implementation of this Policy in their departments.

(b) Deputy Heads

Deputy Heads are accountable for the administration of this Policy in their own department.

**(2) Specific**

(a) Minister of Justice may:

- (i) Make recommendations to the Executive Council on amendments to this Policy.
- (ii) Establish guidelines on the application of this Policy and the development of departmental privacy management programs.

(b) Deputy Minister of Justice may:

- (i) Report to the Minister on the implementation of the Policy and make recommendations on amendments.
- (ii) Provide advice to Deputy Heads on this Policy and the development of departmental privacy management programs.
- (iii) Coordinate effective communication on protection of privacy throughout the GNWT.

(c) Deputy Heads will:

- (i) Promote and implement the Policy within their department.
- (ii) Ensure that the activities of the department are compliant with this Policy and the supporting guidelines.
- (iii) Monitor the effectiveness of the Policy and the guidelines.
- (iv) Designate a member of their Senior Management Team as a Departmental Privacy Officer.

**6. Provisions**

**(1) Privacy Management Program**

Guidelines for developing a privacy management program, privacy training and a Protection of Privacy procedures manual, will be established and maintained by the Department of Justice to support government departments in implementing and promoting good privacy practices based on established privacy standards which,

taken as a whole, will constitute the development of departmental specific privacy management programs.

## **(2) Privacy Breach Reporting**

Upon discovery of a privacy breach, employees must immediately report actual or suspected Privacy Breaches to their Departmental Privacy Officer, who is responsible for reporting the breach to the Deputy Head and program lead.

The Deputy Head, in consultation with the Department of Justice, GNWT Access and Privacy Office, must report the breach to the Information and Privacy Commissioner, in accordance with the Act, if the breach of privacy is considered material.

## **(3) Privacy Impact Assessment**

A privacy impact assessment must be conducted by a public body to determine if a proposed enactment, system, project, program or service that involves the collection, use or disclosure of personal information will meet the requirements of Part 2 (Protection of Privacy) of the Act. A copy of the privacy impact assessment must be provided to the Department's Deputy Minister, and the Department's Privacy Officer, for review or comment.

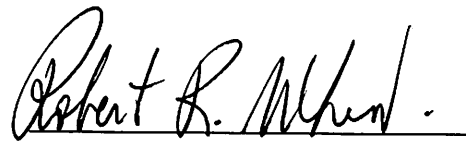
A privacy impact assessment must also be conducted for any proposed common or integrated program or service. This must be submitted to the Information and Privacy Commissioner for review and comment at an early stage of developing the common or integrated program or service.

## **(4) Personal Information Sharing Agreement**

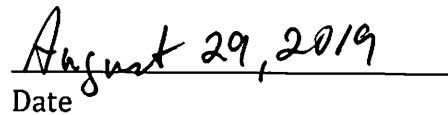
A personal information sharing agreement is required between a department and another department or public body (defined in the *Access to Information and Protection of Privacy Regulations*) or a person or a group of persons, to set out the conditions on the collection, use or disclosure of personal information by the parties to the agreement. These agreements may also be developed with other provincial or territorial governments and their departments.

**7. Prerogative of Executive Council**

Nothing in this Policy shall in any way be construed to limit the prerogative of the Executive Council to make decisions or take action respecting the protection of personal information outside the provisions of this Policy.



Premier and Chairman of the  
Executive Council



Date