

## 4.11 Privacy Policy

### Policy Statement

The Government of Nova Scotia is committed to ensuring that government entities adhere to the privacy protection provisions of the *Freedom of Information and Protection of Privacy Act*, the *Personal Information International Disclosure Protection Act*, and other applicable legislation. Each government entity shall have policies and processes in place to manage and protect personal information at every stage of its life cycle, and shall identify a person responsible for privacy obligations.

### Principles

#### TRANSPARENCY

Each government entity shall have clear policies and practices relating to the management of personal information and shall make these policies and practices readily available.

#### CUSTODIANSHIP

Each government entity is a custodian of an individual's personal information and shall treat the information with due care and attention to the privacy rights and interests of the individual the information is about.

#### SHARED RESPONSIBILITY

All employees of a government entity involved with the handling of an individual's personal information share in the responsibility for protecting personal privacy in accordance with applicable privacy laws and the government entity's policies and practices.

### Definitions

For the purposes of this policy, the following definitions shall apply.

#### INFORMATION LIFE CYCLE

All stages through which information passes between its creation and final disposition, including creation, collection, receipt, maintenance, use, dissemination, and disposition. Functions and activities performed during the life cycle include such things as storage, access/retrieval, and modification.

**DISPOSITION**

Occurs at the final stages of the information life cycle when a record becomes inactive and is either authorized to be securely destroyed, transferred to a public archive, or otherwise addressed in accordance with government legislation and policy.

**EMPLOYEE**

A person retained under any form of employment contract or agreement for a government entity, including members of agencies, boards, commissions or tribunals, students and interns, who have access to records of the government entity.

**GOVERNMENT ENTITY**

All departments, offices of government, public service votes and Crown corporations as listed in Management Manual 100: Management Guide, Chapter 1, Policy 1.2 , .

**FOIPOP (ACT)**

*Freedom of Information and Protection of Privacy Act (NS).*

**PERSONAL INFORMATION**

As defined in clause 3(1)(l) of the *FOIPOP Act*, “recorded information about an identifiable individual, including:

- i) the individual’s name, address or telephone number,
- ii) the individual’s race, national or ethnic origin, colour, or religious or political beliefs or associations,
- iii) the individual’s age, sex, sexual orientation, marital status or family status,
- iv) an identifying number, symbol or other particular assigned to the individual,
- v) the individual’s fingerprints, blood type or inheritable characteristics,
- vi) information about the individual’s health-care history, including a physical or mental disability,
- vii) information about the individual’s educational, financial, criminal or employment history,
- viii) anyone else’s opinions about the individual, and
- ix) the individual’s personal views or opinions, except if they are about someone else”

**PRIVACY BREACH**

Unauthorized collection, access, use, disclosure, storage, or alteration of personal information.

**PRIVACY IMPACT ASSESSMENT (PIA)**

A due diligence process that identifies and addresses potential privacy risks that may occur in the course of the operations of a government entity.

**RECORD**

As defined in clause 3(1)(k) of the *FOIPOP Act*, includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records.

**DEPUTY HEAD**

The position with administrative responsibility for the government entity (e.g. Deputy Minister, Chief Executive Officer, Head of the Public Prosecution Service).

**Policy Objectives**

The policy is designed to ensure that government entities meet their legislated obligations in the management of personal information throughout its life cycle. This includes ensuring the protection of personal information by making reasonable security arrangements against such risks as unauthorized collection, storage, access, use, disclosure or disposition.

**Application**

The policy applies to

- all government entities
- all personal information in the custody or under the control of government entities

**Policy Directives**

1. Each government entity shall have an approved privacy policy and implementation plan, consistent with the template maintained by the Information Access and Privacy Office (Justice), within one year of the effective date of this policy.
2. All existing privacy policies shall be made consistent with this policy within one year of the effective date of this policy.
3. This policy and all privacy policies pursuant to it shall be made available to the public through each government entity's website.
4. Each government entity shall have a process for an individual to request access to their personal information, which will enable them to make a request to correct their personal information.

5. Each government entity shall establish a process for an individual to express concerns about compliance with the privacy policy of the government entity.
6. Each government entity shall ensure that they manage personal information throughout its life cycle only as authorized by law.
7. A government entity may collect, store, access, use, and disclose aggregate information about individuals. Aggregate information shall be compiled and used in a manner that individuals cannot be readily identified.
8. Each government entity shall have a privacy breach protocol in accordance with the template maintained by the Information Access and Privacy Office (Justice).
9. Each government entity shall complete a privacy impact assessment, in accordance with the PIA template maintained by the Information Access and Privacy Office (Justice), for any new program or service, or for a significant change to a program or service, that involves the personal information.
10. A privacy impact assessment shall contain a risk mitigation strategy, the implementation of which shall be monitored by the government entity.
11. Each government entity shall designate an individual responsible for administering and monitoring compliance to the government entity's privacy obligations.
12. The deputy head of each government entity shall identify those individuals responsible for making reasonable security arrangements for personal information in keeping with the provisions of applicable legislation.

### **Policy Guidelines**

1. To aid in the administration of this policy, it is recommended that written procedures concerning the administration of personal information be prepared by the government entity.
2. It is recommended that the individual responsible for administering the privacy policy of the government entity ensure the delivery of privacy awareness training to all employees.
3. Any new or changed initiative, program, procedure, or activity that will involve collection, use or disclosure of or access to personal information should be reviewed with the individual having responsibility for the government entity's privacy obligations
4. The deputy head of a government entity may supplement the requirements of this policy to meet any additional, unique, or special responsibilities a government entity may have to protect personal information.

## Accountability & Security

1. The deputy head of each government entity covered by this policy shall be accountable for compliance with this policy.
2. Each employee is responsible for complying with this policy and the privacy policies of their government entity.

## Monitoring

The Information Access and Privacy Office (Department of Justice) is responsible for monitoring the implementation of this policy.

## References

- *Freedom of Information & Protection of Privacy Act and Regulations*
- *Personal Information International Disclosure Protection Act*
- *Government Records Act*
- Management Manual 300: Common Services, Chapter 4, Policy 4.7 Web Site Privacy Policy
- Management Manual 100: Management Guide, Chapter 1, Policy 1.2 Management Manuals Policy
- Privacy Impact Assessment Template
- Privacy Policy (entity) Template
- Privacy Breach Protocol and Complaint Procedure Template

## Enquiries

Information Access and Privacy Office  
(NS Dept. of Justice)  
PO Box 7  
5151 Terminal Rd., 7th Floor  
Halifax, NS B3J 2L6  
Phone:(902) 424-6836  
Fax: (902) 428-0619

---

*Approval date: April 3, 2008*

*Approved by: Executive Council*

*Manual release date: June 9, 2008*

*Most recent review:*

---

