4.11 Privacy Policy

This policy was approved by Treasury and Policy Board on November 8, 2017. Effective May 8, 2018, this policy replaces the previous 4.11 Privacy Policy and 4.7 Website Privacy Policy.

Policy Statement

The Government of Nova Scotia respects the privacy of individuals and is committed to ensuring that government entities and their employees understand and adhere to the privacy protection provisions of the *Freedom of Information and Protection of Privacy Act* (FOIPOP Act), the *Personal Information International Disclosure Protection Act* (PIIDPA), the *Privacy Review Officer Act* (PRO Act), and other applicable legislation. This policy is part of a program that incorporates privacy as a central component to the day-to-day work of employees.

The FOIPOP Act describes how government entities must collect, use, and disclose personal information. The FOIPOP Act protects the privacy of Nova Scotians by limiting how government manages personal information. Collection, use and disclosure outside of the limits outlined in the FOIPOP Act is prohibited. Government entities are further expected to maintain reasonable security arrangements and procedures to protect against the unauthorized collection, use, disclosure, access or storage of Nova Scotians' personal information.

Definitions

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

CHIEF INFORMATION ACCESS AND PRIVACY OFFICER

Leads the Information Access and Privacy Services Division at the Department of Internal Services and provides overall leadership and strategic direction to government on information access and privacy matters. The Chief Information Access and Privacy Officer is government's designated Chief Privacy Officer.

CONSENT

Is obtained when it is reasonable to expect that the individual providing consent understands the nature, purpose and consequences of the collection, use or disclosure of their personal information to which they are consenting.

EMPLOYEE
A person retained under any form of employment or personal services agreement for a government entity, including members of agencies, boards, commissions or tribunals, students and interns, as well as contractors and service providers, who have access to information under the custody or control of a government entity.

FOIPOP ACT
The *Freedom of Information and Protection of Privacy Act* (Nova Scotia).

GOVERNMENT ENTITY
All government departments, agencies, boards, and commissions categorized as Category I or II entities in Appendix 1-A of the Corporate Administrative Policy Manuals Policy (Policy 1.2 of Chapter 1, Manual 100: Management Guide).

GOVERNMENT RECORDS ACT
The *Government Records Act* (Nova Scotia).

INFORMATION ACCESS AND PRIVACY (IAP) SERVICES
A division within the Department of Internal Services with authority to centralize information access and privacy policies, practices, services and resources for the Government of Nova Scotia.

INFORMATION AND PRIVACY COMMISSIONER
An independent ombudsman appointed by the Governor in Council for a term of five to seven years. The Office of the Information and Privacy Commissioner (OIPC) accepts appeals (referred to as "requests for review") pursuant to the FOIPOP Act and the PRO Act.

PERSONAL INFORMATION
As described in Section 3(1)(i) of the FOIPOP Act, personal information is "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,
ix. the individual's personal views or opinions, except if they are about someone else

PIIDPA
The *Personal Information International Disclosure Protection Act* (Nova Scotia).

PRIVACY BREACH
The intentional or unintentional unauthorized collection, use, disclosure, disposal, modification, reproduction, access, or storage of personal information that is in violation of the FOIPOP Act or PIIDPA.

PRIVACY CHAMPION
An executive-level designate of a government entity that champions and promotes corporate privacy practices within their organization. The Privacy Champion advocates and influences the organization's privacy culture and aligns it with this policy, and works with the Chief Information Access and Privacy Officer to support robust privacy practices across Government.

PRIVACY COMPLAINT
A complaint alleging infringement by a government entity or an employee of an obligation outlined in PIIDPA and the FOIPOP Act's privacy provisions.

PRIVACY DESIGNATE
A designated individual that operationalizes the Privacy Program within a government entity. For most government entities, this designate will hold the title of "IAP Administrator".

PRIVACY IMPACT ASSESSMENT (PIA)
A due diligence exercise that: (i) identifies and addresses potential risks to the privacy of information that may arise during the production of or a change to a system, project, program or activity of a government entity; and (ii) helps to ensure a government entity's compliance with this policy, the FOIPOP Act and PIIDPA.

PRIVACY NOTICE
A notification, electronic or otherwise, to individuals about: (i) the purpose for which personal information is collected; (ii) the authority for such collection; (iii) how the information will be used; and (iv) whether the information will be disclosed to another government entity or third party, and the reason for such disclosure.

PRIVACY PROGRAM
The program encompasses privacy controls and processes, mechanisms for monitoring, tools for fulfilling privacy obligations, and provides awareness and education of privacy best practices through training.

PRIVACY PROVISIONS
Sections 24 to 31 of the FOIPOP Act.

PRIVACY STATEMENT
A statement provided to individuals that summarizes the information practices that are applied by the entity and its employees, in the format made available by IAP Services.

PRO ACT
The *Privacy Review Officer Act.*

Policy Objectives

This policy is designed to assist government entities in the proper and lawful management of personal information by:

- establishing a culture of privacy that respects individuals' right to privacy and emphasizes appropriate personal information handling best practices.
- setting out rules, principles and practices as they relate to privacy and the management of personal information.
- providing education, training and tools to their employees to aid in creating a corporate environment that fully incorporates privacy into its operations.
- providing avenues for individuals to challenge the compliance of government entities' privacy practices and applications of this policy to foster public trust.

Application

The policy applies to

- all employees,
- all government entities, and
- all personal information in the custody or under the control of government entities.

Policy Directives

PERSONAL INFORMATION PRACTICES

General

1. Personal information must be collected, used, disclosed and managed in accordance with the FOIPOP Act and the FOIPOP Act's associated regulations, to the extent that the FOIPOP Act and its regulations apply to such collection, use, disclosure or management.
2. Government entities shall, to the extent reasonably possible:
   a. limit the collection, use, and disclosure of personal information to the minimum amount necessary.
   b. provide a timely, program-specific Privacy Notice where there is direct collection of personal information. The location of the Privacy Notice and its content must be determined by the program owner, in consultation with IAP Services.
   c. government entities' websites must include a Privacy Statement.
   d. limit access to personal information to only those employees who need to know the information to carry out their duties for the government entity.
   e. undertake reasonable efforts to prevent the unauthorized collection, use, disclosure and disposal of personal information.
   f. access or store personal information under their custody or control in accordance with PIIDPA.
   g. obtain, if and when required, consent from individuals if such individuals' personal information will be collected, used or disclosed by the government entity.
   h. maintain an inventory of personal information holdings that identifies, at a minimum, the system owner (if the information is held in a system), a description of the personal information held, and the location and authority for collecting the information.
   i. ensure that any information sharing and research agreements to be entered into by the government entity are reviewed by the applicable privacy designate.
3. Unauthorized access, collection, use or disclosure of personal information by an employee may result in disciplinary action.

Accuracy of Personal Information

1. Government entities shall undertake reasonable efforts to ensure that all personal information held by the government entity, and which is to be used in any decision-making process affecting an individual, is as accurate, up-to-date and complete as possible.

2. Government entities shall undertake reasonable efforts to collect personal information directly from the individual to whom the information relates.

Protecting Personal Information

1. Government entities shall undertake reasonable efforts to protect personal information from access or use by unauthorized third parties, by implementing reasonable administrative, technical and physical safeguards against such access or use. Such safeguards may be prescribed by the Department of Internal Services.
2. A system administered by a government entity which stores personal information shall, to the extent reasonably and technically feasible, include audit logs that track access to personal information. Audit logs must be made available to any privacy designate upon request for the purposes of a breach or complaint investigation.
3. Employees of government entities who prepare or manage contracts that involve the collection, use, storage or access of personal information by any third party shall consult with legal counsel, and shall ensure that privacy protection provisions recommended by counsel are included in such contracts.

Retention and Destruction of Personal Information

1. Government entities shall develop retention schedules for the management of records which may contain personal information in accordance with the *Government Records Act.*
2. Personal information held on electronic media must always be disposed of in accordance with the Electronic Media Disposal Standard, or other comparable industry standard accepted by the Department of Internal Services.
3. Personal information contained in hard copy format must be disposed of in accordance with standards governing the destruction of paper records as defined by the Records Management Policy or, in the alternative, by destroying such records in such manner so that no personal information can be derived from these records following their disposal.

Correction to Personal Information

1. Upon receiving a request for correction of personal information pursuant to Section 25 of the FOIPOP Act, government entities shall, where reasonably possible, respond to the request within thirty calendar days.

PRIVACY TRAINING

1. All employees of a government entity shall complete mandatory privacy awareness training once every two years.
2. New employees of a government entity shall complete mandatory privacy awareness training within their first three months of employment.

PRIVACY IMPACT ASSESSMENTS

1. Government entities shall notify their privacy designates upon any development of or change to any system, project, program, service or activity that involves the collection, use, storage, disclosure or access of personal information, to obtain an opinion on whether a privacy impact assessment (PIA) is necessary.
2. Government entities shall conduct privacy impact assessments (PIAs), if and to the extent required, in accordance with IAP Services' practices, procedures and documentation for PIAs.
3. IAP Services must be engaged in the development of any PIA where a system, project, program, service or activity that involves the collection, use, storage, disclosure or access of personal information is developed, owned, managed or shared by more than one government entity.
4. Where possible, PIAs must be completed and approved by the deputy or head of the government entity, before any personal information is collected, used, stored, disclosed or accessed.
5. Each government entity that has a Memorandum of Understanding with IAP Services shall provide signed copies of all PIAs to IAP Services for purposes of reporting and monitoring compliance under the Privacy Program.
6. The Information and Privacy Commissioner's Office may be notified of certain PIAs based on such PIAs' scope and complexity of the system, service, program or activity and pursuant to the Privacy Impact Assessment Process.

PRIVACY BREACHES

1. Employees shall immediately report actual or suspected privacy breaches to their supervisor.
2. Supervisors shall report actual or suspected breaches to the applicable privacy designate.
3. All breaches shall be investigated by the government entity's privacy designate in accordance with the Privacy Breach Protocol made available by IAP Services.
4. Each government entity that has a Memorandum of Understanding with IAP Services shall report annually to IAP Services on the number of privacy breaches that have occurred for the purposes of reporting and monitoring compliance under the Privacy Program.
5. The Information and Privacy Commissioner's Office may be notified of privacy breaches by IAP Services, based on such breaches' severity and pursuant to the Privacy Breach Protocol.

PRIVACY COMPLAINTS

1. Upon receipt of a privacy complaint, government entities shall refer such complaint to the applicable privacy designate.
2. All complaints shall be investigated by the government entity's privacy designate in accordance with a privacy complaints protocol made available by IAP Services.
3. Government entities shall respond to the complainant within a reasonable time frame, and where possible, within thirty calendar days.

Policy Guidelines

To aid in the administration of this policy, government entities may develop additional written procedures to support its implementation and their specific needs. These procedures must be in alignment with the direction of this policy and the Privacy Program. The government entity may choose to consult with IAP Services on these procedures.

Accountabilities

Deputy or other heads (e.g. CEOs) shall:

- Designate a Privacy Champion within their respective organization.
- Ensure implementation of this policy and any supporting procedures, guidelines and tools made available by IAP Services.
- Approve PIAs, research agreements and information sharing agreements.
- Ensure privacy breaches are reported to IAP Services.

Responsibilities

SENIOR MANAGEMENT

Senior management shall:

- Communicate this policy to all employees within their organization.
- Ensure that employees complete all mandatory training on privacy in accordance with the timelines set out in this policy.

PRIVACY CHAMPIONS

Privacy champions shall:

- Work in partnership with the Chief Information Access and Privacy Officer to support and implement the Privacy Program in their organization.
- Act as an advocate for privacy awareness and best practices within their organization.

PRIVACY DESIGNATES

Privacy designates shall:

- Act as a liaison and subject matter expert for government entities and assist with compliance under this policy.
- Participate in the development of PIAs, information sharing agreements and research agreements.
- Conduct investigations into privacy breaches and privacy complaints.

EMPLOYEES

Employees shall:

- Comply with this policy and any supporting procedures, guidelines and tools made available by IAP Services.
- Immediately report actual or suspected privacy breaches to both supervisors and applicable privacy designates, including privacy complaints, as per IAP Services' privacy breach and privacy complaints protocols.
- Complete all mandatory privacy awareness training.

CHIEF INFORMATION ACCESS AND PRIVACY OFFICER

The Chief Information Access and Privacy Officer shall:

- Set the vision and strategic direction for government information access and privacy. They will be the designated Chief Privacy Officer for the Government of Nova Scotia.
- Advise and consult with heads of government entities and privacy champions regarding issues that may affect corporate privacy practices and compliance with this policy.

IAP SERVICES

IAP Services shall:

- Establish and deliver Government's Privacy Program, including associated processes, guidelines and tools that leads to a culture of privacy for all government entities.
- Develop and make available privacy awareness training and monitor completion of such training.
- Create and maintain current protocols and processes for completing PIAs, privacy breach and complaint reports, as well as develop and issue any other guidelines, procedures and templates that are necessary to fulfill the privacy obligations outlined in this policy.
- Develop metrics and report statistics on the of number of breaches, complaints, training sessions and PIAs completed.

Monitoring

The Information Access and Privacy Services Division of the Department of Internal Services is responsible for monitoring the implementation of this policy and for reviewing and updating it regularly.

References

LEGISLATION

- *Freedom of Information and Protection of Privacy Act* and Regulations (FOIPOP Act)
- *Government Records Act* (GRA)
- *Personal Information International Disclosure Protection Act* and Regulations (PIIDPA)
- *Privacy Review Officer Act* (PRO Act)

RELATED DOCUMENTS

- Corporate Administrative Policy Manuals
- Electronic Media Disposal Standard
- Government Records Management Policy
- Privacy Breach Protocol
- Privacy Complaint Protocol
- Privacy Impact Assessment Process

Enquiries

Information Access and Privacy (IAP) Services
NS Department of Internal Services
PO Box 72
5161 George St. 12th Floor
Halifax NS B3J 2L4
902-424-2985
iapservices@novascotia.ca

Approval date:	***November 8, 2017***	Effective date:	***May 8, 2018***
Approved by:	***Treasury and Policy Board***	Administrative update:	