

Privacy Policy

**Executive Council Office
Treasury Board Office
Office of Policy and Priorities
Chief Information Office**

POLICY STATEMENT

It is the policy of the Executive Council Office, Treasury Board Office, Office of Policy and Priorities, and the Chief Information Office that adherence to the privacy protection provisions of the *Freedom of Information and Protection of Privacy Act*, the *Personal Information International Disclosure Protection Act*, the *Government Privacy Policy*, the *Privacy Review Office Act*, and other applicable legislation will be ensured. The offices will uphold the principles of transparency, custodianship and shared responsibility established in the *Government Privacy Policy*, as it relates to the collection, use and disclosure of personal information.

DEFINITIONS

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

employee an individual in the employ of, seconded to, or under personal service contract to the Executive Council Office, Treasury Board Office, Office of Policy and Priorities, or the Chief Information Office and their volunteers, students and interns who have access to records.

FOIPOP *NS Freedom of Information and Protection of Privacy Act*

office(s) refers to the Executive Council Office, Treasury Board Office, Office of Policy and Priorities, and the Chief Information Office

personal information

as defined in clause 3(1)(1) 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	the event of unauthorized collection, access, use, disclosure, or alteration of personal information
PIA	a Privacy Impact Assessment is a due diligence exercise which identifies and addresses potential privacy risks that may occur in the course of the operations of a public body
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

POLICY OBJECTIVES

The policy is designed to ensure that government meets its 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 access, collection, use, disclosure or disposal.

APPLICATION

This policy applies to:

- all employees of the Executive Council Office, Treasury Board Office, Office of Policy and Priorities, and the Chief Information Office
- all personal information in the custody and control of the Executive Council Office, Treasury Board Office, Office of Policy and Priorities, and the Chief Information Office

POLICY DIRECTIVES

- The office shall collect, access, store, use, disclose and dispose of personal information only where authorized by law or agreement with other public body that is authorized by law.
- The heads of the offices shall identify those individuals with designated or delegated responsibilities for making reasonable security arrangements for personal information in keeping with the provisions of applicable legislation.
- The office shall have a privacy breach protocol, per the template maintained by the NS Information Access and Privacy Office (see Appendix A).
- The office shall complete a privacy impact assessment for any new program or service or for a significant change to a program or service, as per the template maintained by the NS Information Access and Privacy Office (see Appendix B).
- All employees shall be advised of the policy coming into force.
- This policy shall be made readily available and will be posted on the offices websites.
- Requests for correction of personal information or to express concern regarding compliance shall be directed to the Corporate IAP/FOIPOP Administrator, Executive Council Office.

POLICY GUIDELINES

To support the policy in securing Personal Information, the offices will establish specific procedures that will include the following:

- Personal Information will be used, disclosed, or shared only for the purpose for which it was obtained or compiled, or for a use compatible with that purpose [pursuant to Sections 24-30, *FOIPOP Act*; also see “Privacy Impact Assessment Template and Guide”, p. 15-16]
- Access to files containing Personal Information will be limited to access needed for operational requirements / performance of duties, pursuant to Section 27, *FOIPOP Act*
- Databases containing Personal Information will be password-protected
- Directories containing Personal Information will be password-protected
- Passwords will be issued on a need-to-know basis, as determined by operational requirements, pursuant to Sections 27, *FOIPOP Act*
- Filing cabinets containing Personal Information will be locked
- Personal Information will not be stored on thumb drives
- Files containing Personal Information will not be removed from offices or left unattended
- Blackberries will be password-protected and emails sent and received using Group Wise software will be encrypted by the Governmental Blackberry server
- Approval is required from the head of a public body to take Blackberries and other electronic devices outside the country, pursuant to Section 9(4) of the *Personal Information International Disclosure Protection Act (PIIDPA)* See also Appendix B, “Privacy Impact Assessment Template and Guide,” p. 17-19]
- When sending e-mails to more than one private individual at a time, when those individuals are known to the sender but unknown to each other, ensure that the individuals are blind copied. This will ensure that their e-mail addresses are not inappropriately disclosed to all the other third parties in the e-mail, and will therefore prevent a privacy breach from occurring.
- When an office receives a request from a third party to assist in resolving a problem with another third party, ensure compliance with s. 27 of the act (i.e. ensure that the office has the permission of the first third party, in writing, to share his/her Personal Information with the second third party)
- If this authority cannot be obtained, where possible the office will provide the contact information for the first third party to contact the second third party directly
- disposal of both transitory or master records containing Personal Information will be carried out only using secure methods, such as shredding (including shred boxes used for on-site confidential shredding)
- Training and awareness will be provided to all staff on the privacy protection of Personal Information.
- the offices shall ensure that all new employees receive a copy of this policy in an orientation package, and that the Corporate IAP / FOIPOP Administrator will provide training on proper procedures regarding the privacy of Personal Information.
- the offices will provide a process for expressing concerns about compliance with its privacy policy.
- This process will include information on how to contact the Corporate IAP / FOIPOP Administrator, what detail the Administrator needs in order for the offices to provide an appropriate response, as well as the time frame in which the individual can expect to receive a response.

ACCOUNTABILITY & SECURITY

1. The deputy head of each office shall be accountable for compliance with this policy.
2. Each employee of each office is responsible for complying with this policy and the privacy policy of the government of Nova Scotia.

MONITORING

The Corporate IAP / FOIPOP Administrator for the Executive Council Office will be responsible for monitoring compliance with this policy.

REFERENCES

- *Freedom of Information and Protection of Privacy Act* and regulations
- *Personal Information International Disclosure Protection Act*
- *Government Records Act*
- *Privacy Review Officer Act*
- Management Manual 300: Common Services, Chapter 4, Policy 4.7, Website Privacy Policy
- Management Manual 300: Common Services, Chapter 4, Policy 4.11 Privacy Policy
- Management Manual 100: Management Guide, Chapter 1, Policy 1.2 Management Manuals Policy
- Privacy Impact Assessment
- Privacy Breach Protocol
- Canadian Standards Association Model Code 10 Principles

ENQUIRIES

Corporate IAP/FOIPOP Administrator
Executive Council Office
902-424-4879 (direct)
902-424-8910 (general)
902-424-0667 (fax)

Approval Date: **March 19, 2009**
Effective Date: **April 1, 2009**
Revised: **January 18, 2010**

Approved By:

Secretary to/Clerk of
Executive Council,
Executive Council Office

Deputy Minister,
Office of Policy and
Priorities

Deputy Minister,
Treasury Board

Chief Information Officer,
Chief Information Office