

Department of Natural Resources

Privacy Policy

Approval date: September 2009

Effective date: September 2009

Approved by: Peter Underwood

I. POLICY STATEMENT

The Department of Natural Resources is committed to ensuring the privacy protection provisions of the *Freedom of Information and Protection of Privacy Act (FOIPOP)*, *Personal Information International Disclosure Protection Act (PIIDPA)*, the Government Privacy Policy and other applicable legislation and policies. The Department 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.

2. DEFINITIONS

For the purposes of this policy, the following definitions will apply. These definitions are not to be construed as over-riding any statutory definitions provided in legislation.

employee an individual in the employ of, seconded to, or under personal service contract to the Department, including its agencies, boards, commissions or tribunals and their volunteers, students, and interns who have access to records

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

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 the event of unauthorized access or inappropriate 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 the department or its agencies, boards or commissions
- 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”
- records life cycle** the stages of activity from creation/receipt of a record up to and including its final disposition. Activities in the records life cycle include creation, receiving, classifying, indexing, registering, maintaining, accessing, retrieving, using, distributing, storing, migrating to another medium, destroying and preserving
- third party** in relation to personal information, means any individual, group of individuals, or organization other than the person whom the personal information is about, or a department or entity

3. **POLICY OBJECTIVES**

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

4. **APPLICATION**

The policy applies to:

- all employees of the Department as defined in this policy; and
- all personal information in the custody and control of the Department.

5. **POLICY DIRECTIVES**

- a. Personal information will be collected, accessed, used, stored, disclosed and disposed of, in compliance with the law.
- b. The policy will be made readily available and will be posted on the Department’s Internet website.
- c. Requests for correction of personal information and concerns about compliance, will be directed to the Manager, Information Management & Information Access & Privacy (IAP).
- d. Privacy Impact Assessments will be completed for any new program or

- service or for a significant change to a program or service.
- e. The Department will have a privacy breach protocol.
 - f. Program areas will take responsibility for ensuring that contracts with service providers are compliant with this policy and the *Personal Information International Disclosure Protection Act*.
 - g. All existing privacy policies of the department will be consistent with this policy and the corporate privacy policy.
 - h. The Department may collect, use, and disclose aggregate information about individuals for statistical purposes, and this information will be compiled and used in a way such that individuals cannot readily be identified.
 - i. Personal information will be disposed of in accordance with approved records retention schedules.
 - j. The Department will make reasonable security arrangements to protect personal information in its custody and under its control in keeping with the provisions of applicable legislation.
 - k. The Department will ensure best practices, as established by each branch, are followed in the housing and storage of personal information.
 - l. The Department will prepare a Privacy Procedures Manual that addresses the specific privacy needs of the various Branches and Divisions, including a process to correct personal information and for expressing concerns about compliance with the policy.

6. POLICY GUIDELINES

- All employees will be advised of the policy coming into force.
- Training and awareness on the privacy protection of personal information should be delivered to all staff regularly or as requested, depending on specific needs.
- All new employees will receive a copy of the policy in an orientation package and if required will receive training on proper procedures regarding the privacy of personal information.

7. ACCOUNTABILITY & SECURITY

The Department of Natural Resources is accountable for the privacy of the personal information it holds, and for the associated business processes and procedures for the collection, use, disclosure, retention and disposal of that information.

Accountability

The Deputy Minister is responsible for:

- a. ensuring compliance with the corporate policy
- b. approval and compliance of this policy

Senior Management is responsible for:

- a. approving the policy and any amendments
- b. ensuring the annual review of the policy is conducted
- c. ensuring communication of the corporate and Department policies within their branches

Directors / Managers / Supervisors are responsible for:

- a. ensuring that all employees are trained and understand the policy
- b. ensuring that all existing and new employees are notified that a copy of the policy is on the Department's website
- c. participating in the annual review of the policy
- d. resolving any privacy breaches

Manager, Information Management & IAP is responsible for:

- a. establishing guidelines and procedures for administering the policy
- b. processing requests and concerns about compliance with this policy as well as requests for the correction of personal information
- c. providing training and awareness on privacy protection of personal information to staff
- d. participating in the completion of privacy impact assessments
- e. participating in the resolution of privacy breaches
- f. coordinating the review of the policy

Employees are responsible for:

- a. complying with the Department's privacy policy and procedures
- b. participating in training and awareness sessions
- c. understanding the policy and how it impacts their work

Security

The Department will make every reasonable effort to ensure that appropriate security protocols are implemented to protect the confidentiality, integrity, availability of personal information through mechanisms including, but not limited to:

- the use of locked filing cabinets or areas with restricted secure access to store sensitive information
- the use of access permission levels on electronic systems used to manage personal information
- the use of passwords to protect personal information in electronic systems
- access to personal information will be limited to individuals who need access for the purpose of carrying out a program or service
- timely and secure disposal of both transitory or master records containing personal information

8. MONITORING

The Manager, Information Management and IAP will monitor the implementation of the policy. The results of the reviews and recommendations will be communicated to Senior Management.

Managers and supervisors will monitor their staff to ensure compliance with the policy.

9. REFERENCES / AUTHORITY

NS Freedom of Information & Protection of Privacy Act (FOIPOP) and Regulations
Personal Information International Disclosure Protection Act (PIIDPA) and Regulations

Government Records Act

Government Website Privacy Policy, June 1, 2004

Management Manual 100: Management Guide, Chapter 1, Policy 1.2 Management Manuals Policy

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

Canadian Standards Association Model Code 10 Principles

Department of Natural Resources Records Management Policy

Department of Natural Resources Privacy Impact Policy

10. INQUIRIES

Inquiries regarding this policy should be directed to the Manager, Information Management and IAP, Valerie Brisco (902) 424-1580 vjbrisco@gov.ns.ca