

**POLICY TITLE:** Privacy Policy

**POLICY STATEMENT:** Nova Scotia Business Inc. (NSBI) is committed to ensuring it fulfils its protection of privacy obligations and manages personal information in accordance with the requirements of the *Freedom of Information and Protection of Privacy (FOIPOP) Act*, the *Personal Information International Disclosure Protection Act (PIIDPA)*, the Canada Anti-Spam Legislation (CASL) and applicable Government of Nova Scotia policies related to personal privacy.

**PURPOSE / OBJECTIVE:** The objectives of the NSBI Privacy Policy (this Policy) are:

- to ensure NSBI achieves compliance with applicable privacy laws and policies and appropriately manages personal information throughout the record life cycle.
- to ensure employees, officers and service providers of NSBI are aware of and fulfil their respective protection of privacy responsibilities.

This Policy and its interpretation are guided by the following privacy principles:

**Custodianship:** NSBI is a custodian of an individual's personal information and treats it with due care and attention to the privacy rights and interests of the individual the information is about and in accordance with applicable privacy laws and policies.

**Shared Responsibility:** All employees, officers and service providers of NSBI share in the responsibility for protecting personal privacy.

**Transparency:** NSBI's policies and practices relating to the management of an individual's personal information must be clear and made readily available to the individual.

**DEFINITIONS:** (see **Appendix 1**)

**APPLICATION:** The NSBI Privacy Policy (this Policy) applies to:

- officers and employees of NSBI; and
- personal information in the custody or under the control of NSBI but not to personal information in records to which the *FOIPOP Act* and *PIIDPA* do not apply, including :
  - published material,
  - material that is available for purchase by the public, or
  - material that is a matter of public record

## **POLICY DIRECTIVES:**

### **1. General**

Personal information in the custody or under the control of NSBI is to be managed in compliance with the *Freedom of Information and Protection of Privacy (FOIPOP) Act* and the *Personal Information International Disclosure Protection Act (PIIDPA)*, the Canada Anti-Spam Legislation (CASL) and consistent with applicable Government of Nova Scotia policies related to personal privacy.

### **2. Collecting Personal Information**

Personal information may only be collected if it relates directly to and is necessary for an operating program or activity of NSBI, or if expressly authorized or required by law.

### **3. Using / Disclosing Personal Information**

Personal information may only be used and / or disclosed:

- a) for the purpose for which it was obtained or compiled, or a use that has a reasonable and direct connection to that purpose,
- b) with the individual's informed written consent,
- c) to collect a debt from or make a payment to an individual, or
- d) if otherwise expressly authorized or required by law.

### **4. Using Personal Information to Send a Commercial Electronic Message**

In addition to the requirements of Policy Directive 3 (above), a person's electronic address must not be used to send the person a commercial electronic message (CEM) unless:

- a) The CEM is an excluded class of CEM under CASL; or
- b) Where:
  - i. NSBI has the person's expressed or implied consent to receive the CEM;
  - ii. the electronic message clearly identifies NSBI (or NSBI's service provider) as the sender of the message and includes the contact information for NSBI (or NSBI's service provider); and
  - iii. the electronic message includes an unsubscribe mechanism.

An unsubscribe request must be acknowledged and implemented no later than 10 business days after the request has been sent.

## 5. Disclosing Personal Information Outside Canada

In addition to the requirements of Policy Directive 3 (above), personal information may only be disclosed outside Canada:

- a) with the individual's informed written consent,
- b) to collect a debt from or make a payment to an individual,
- c) if otherwise expressly authorized under *PIIDPA*, or
- d) if the personal information is business contact information and the disclosure outside Canada is for the purpose for which the business contact information was obtained or compiled, or a use that has a reasonable and direct connection to that purpose.

## 6. Accuracy of Personal Information

Where an individual's personal information will be used to make a decision that directly affects the individual, every reasonable effort must be made to ensure the personal information is accurate and complete.

## 7. Minimum Retention After Use

Where an individual's personal information is used to make a decision that directly affects the individual, the information must be retained for at least one year after the use so the individual has a reasonable opportunity to request access to his or her personal information and request a correction if the individual believes there is an error or omission.

## 8. Protecting Personal Information

### Security arrangements:

Reasonable security arrangements are to be made to protect personal information throughout the record life cycle from such risks as unauthorized collection, use, disclosure, access, storage and disposal.

### Website privacy protections:

The Government of Nova Scotia Website Privacy Policy and the Government of Nova Scotia Cookie Notification Standard apply to the operation of NSBI websites. Further and complementary to these provisions:

- a) Where personal information is being collected using a web-based tool, secure connections must be used and the following prominently displayed at the initial point of collection:
  - i. The purpose for the collection of personal information (i.e. the purpose for use and disclosure); and
  - ii. How one can obtain access to or request a correction of their personal information collected through that site.
- b) Personal information about a minor (i.e. less than 19 years of age) will not knowingly be published on the NSBI website without the written consent of the minor's parent or legal guardian.

### Foreign demand for disclosure protections:

**Access / storage outside Canada:** Personal information may only be accessed from, or stored outside Canada:

- a) with the individual's informed written consent,
- b) for the purpose of disclosing personal information where disclosure outside Canada is allowed under *PIIDPA*, or

- c) if approved by the Head, NSBI, and reported to the Nova Scotia Minister of Justice in a “Form 1” report.

**Transport outside Canada:** Personal information may only be temporarily transported outside Canada in a mobile electronic device:

- a) if approved by the Head, NSBI, or
- b) by an officer or employee of NSBI where:
  - i. NSBI has issued the officer or employee the mobile electronic device,
  - ii. the officer or employee is authorized to travel outside Canada for NSBI business purposes, or required, implicitly or explicitly, to perform work responsibilities while travelling outside of Canada for other purposes, and
  - iii. the officer or employee is authorized to travel outside Canada for NSBI business purposes, or required, implicitly or explicitly, to perform work responsibilities while travelling outside of Canada for other purposes,
  - iv. there is a reasonable expectation that the personal information is necessary for the officer’s or employee’s performance of duties during the period of travel outside Canada, and
  - v. the personal information is protected from unauthorized access and disclosure in accordance with the NSBI Code of Conduct, the NSBI Oath or Solemn Affirmation of Office and other data protection policies and procedures that may apply.

**Notice of foreign demand:** An officer, employee or service provider of NSBI must immediately notify the Nova Scotia Minister of Justice and the Head, NSBI, of the receipt of a known or suspected **foreign demand for disclosure** of personal information or of a known or suspected unauthorized disclosure of personal information in response to a foreign demand for disclosure. Persons acting in good faith and on a reasonable belief shall not be punished or disadvantaged for having given such notice.

#### Privacy impact assessment

NSBI shall have and maintain a privacy impact assessment (PIA) process and template consistent with the template maintained by the Information Access and Privacy Services Division of the Department of Internal Services.

Subsequent to this Policy coming into effect, a PIA is to be conducted for any new NSBI program or service or a significant change to an NSBI program or service that involves the collection, use or disclosure of personal information.

#### Privacy breach protocol

NSBI shall have and maintain a privacy breach protocol consistent with the privacy breach protocol template maintained by the Information Access and Privacy Services Division of the Department of Internal Services.

The NSBI privacy breach protocol must be followed in the event of a known or suspected privacy breach.

## 9. Individual Access

Individuals have the right under the *FOIPOP Act* to make an application for access to their personal information in the custody or under the control of NSBI and, if the applicant believes there is an error or omission, to make an application for a correction of that information. All applications under the *FOIPOP Act* are to be directed without delay to IAP Services, for coordination of processing and response.

## 10. Transparency

This Policy shall be available to the public and posted on the NSBI website.

## 11. Complaints and Appeals

NSBI shall have and maintain a process for an individual to register a formal complaint about the treatment of his or her personal information under the custody or control of NSBI. All formal privacy complaints are to be directed without delay to IAP Services, for coordination of investigation and response.

## 12. Contracting

Where a service provider will be contracted to collect, use, disclose, store, access or dispose personal information on behalf of NSBI, the contract must specifically address the management of the personal information to enable the service provider to comply with the *FOIPOP Act*, *PIIDPA*, *CASL* and this Policy in performing services for NSBI.

## 13. Other

NSBI may collect, use, access, store and disclose aggregated information about a group of individuals. Aggregated information must be compiled and used in a manner that there is no reasonable expectation an individual could be identified.

## POLICY GUIDELINES:

### 1. Collecting Personal Information

The purpose for the collection of personal information (i.e. the intended purposes for use and disclosure of the personal information) should be identified at or before the time personal information is collected.

### 2. Retention of Personal Information

Personal information should not be kept longer than is necessary to fulfil the purpose for which the personal information was collected, the minimum retention requirements of this Policy (see Policy Directive #7above), the approved retention schedule for the record and other legal obligations.

### 3. Privacy Procedures

Where an NSBI program or service involves the collection, use, or disclosure of personal information, written privacy procedures for the management and protection of personal information should be prepared.

### 4. Privacy Training

Officers and employees who are to handle personal information in performing their job function are to be given training about this Policy and other applicable privacy procedures before being given access to the personal information.

Additionally, the Provincial Privacy Policy requires all employees of departments and crowns to have training every three years.

**ACCOUNTABILITIES:**

**President & CEO** – is the approval authority for this Policy, including its amendment or rescindment.

**Head, NSBI** – has overall accountability for NSBI's compliance with the *FOIPOP Act* and *PIIDPA* and is the approval authority for:

- decisions under the *FOIPOP Act* including personal information access and correction applications; and
- decisions under *PIIDPA* including authorizing storage, access and temporary transport of personal information outside Canada.

**Executive Team** – is responsible for:

- promoting this Policy.

**Director, Corporate Services & Compliance** – is responsible for:

- overseeing implementation of this Policy including its interpretation;
- ensure privacy training forms part of new employee orientation and regular three-year rotation training for all employees occurs; and
- monitoring compliance with this Policy.

**Information Access and Privacy Services (IAP Services)**– is responsible for:

- day to day implementation of this Policy;
- coordinating responses to personal information access and correction applications made under the *FOIPOP Act*; and
- coordinating investigations and responses to formal privacy complaints.

**Webmaster** – is responsible for:

- implementing and monitoring compliance with the website privacy protections of this Policy.

**Unit Heads** – are responsible for:

- ensuring the programs and services delivered by their business unit are conducted in a manner consistent with this Policy and applicable privacy laws.

**Supervisors** – are responsible for:

- ensuring that the employees they supervise are aware of this Policy and their responsibilities under this Policy.

**Officers and employees** – are responsible for:

- following this Policy;

- attending privacy training that may be required; and
- contacting their supervisor or IAP Services, when they have questions or concerns about a privacy matter.

**EXCEPTIONS:** Exceptions to this Policy may be approved by a member of the Executive Team.

**MONITORING:** The Director, Corporate Services & Compliance is responsible for monitoring this Policy’s implementation and for its scheduled review.

This Policy shall be reviewed every three years.

**REFERENCES:**

- *Freedom of Information and Protection of Privacy Act / Regulations*
- *Privacy Review Officer Act*
- *Personal Information International Disclosure Protection Act / Regulations*
- Canada Anti-Spam Legislation (CASL) / Regulations
- Government of Nova Scotia Management Manual 300: Common Services, Chapter 4, Information and Records Management Services:
  - Policy # 4.7 – Website Privacy Policy (and appended “Website Privacy Policy Statement”)
  - Policy # 4.9 – Citizen Online Identity Authentication Policy
  - Policy # 4.10 – Information Management Policy
  - Policy # 4.11 – Privacy Policy
- Government of Nova Scotia, Cookie Notification Standard
- Code of Conduct – NSBI Employees
- NSBI Oath or Solemn Affirmation of Office
- NSBI Privacy Impact Assessment Guide and Template
- NSBI Privacy Compliant Process
- NSBI Privacy Breach Protocol Guide and Template
- NSBI Information and Communications Technology Policy

**APPENDICES:** Appendix 1: Definitions

**ENQUIRIES:** For more information about this policy please contact:  
 Director, Corporate Services & Compliance  
 Nova Scotia Business Incorporated  
 PO Box 2374  
 Halifax, NS B3J 3E4  
 Tel: (902) 424-6650

Toll free in Nova Scotia: 1-877-297-2124  
Toll free in North America: 1-800-260-NOVA (6682)  
E-mail: info@nsbi.ca

---

<b>APPROVED BY:</b>	President & CEO
<b>APPROVAL DATE:</b>	June 1, 2019
<b>EFFECTIVE DATE:</b>	June 1, 2019
<b>REPLACES:</b>	POL-IM-3.0 June 1, 2016
<b>NEXT REVIEW DATE:</b>	June 1, 2022

---

Approved: original signed by:  
Laurel Broten, President & CEO



## Appendix 1

### DEFINITIONS

Business contact information	means information to enable an individual who represents a business or social enterprise to be contacted and includes the individual's name, position title, direct telephone number, mobile phone number, and e-mail address.
Canada Anti-Spam Legislation (CASL)	means the federal Canadian statute titled "An Act to promote the efficiency and adaptability of the Canadian economy by regulation certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act".
Commercial activity	means as defined in Section 1. (1) CASL, which currently defines it as " <i>any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, whether or not the person who carries it out does not in the expectation of profit, other than any transaction, act or conduct that is carried out for the purposes of law enforcement, public safety, the protection of Canada, the conduct of international affairs or the defence of Canada</i> ".
Commercial electronic message (CEM)	means as defined in Section 1.(1) of the Canada Anti-Spam Law (CASL), which can generally be summarized as meaning an electronic message that " <i>encourages participation in a commercial activity</i> ", including an electronic message that: <ul style="list-style-type: none"><li>• offers to buy, sell, exchange or lease a product, goods or service, land or interest / right in land;</li><li>• offers to provide a business or investment opportunity; or</li><li>• advertises or promotes these things, or</li><li>• promotes a person, including the public image of a person, as being one who does these things; and</li><li>• includes a request for consent to send a CEM.</li></ul>
Electronic address	means as defined in Section 1.(1) CASL, which currently defines it as " <i>an address used in connection with the transmission of an electronic message to an e-mail account, an instant messaging account, a telephone account or any similar account</i> ".

Electronic message	means as defined in Section 1.(1) CASL, which currently defines it as “a message sent by any means of telecommunication including a text, sound, voice or image message”.
Employee	means a permanent, casual or term employee, a co-op student, a student placement or intern, a volunteer, or a person under a personal services contract or temporary work assignment with NSBI.
Excluded class of CEM	<p>means a category of CEM that pursuant to CASL has been prescribed as not subject to Section 6 of CASL (the provision that restricts the sending of a CEM). The following are examples of some of the excluded classes of CEM’s:</p> <ul style="list-style-type: none"> <li>• a CEM to a person engaged in a commercial activity and the CEM is an inquiry or application related to that activity;</li> <li>• a CEM that is a quote, estimate or response to a request;</li> <li>• a CEM that completes, confirms a commercial transaction the recipient agreed to enter into</li> <li>• a CEM that delivers a product, goods, service, update / upgrade the recipient is entitled to receive under the terms and conditions of an existing transaction;</li> <li>• a CEM that is warranty information, product recall information, safety or security information about a product, goods, service ordered under a subscription, membership, account or loan;</li> <li>• a CEM that is an ongoing subscription, membership, account or loan;</li> <li>• a CEM to employees, or to employees about an employee benefit plan.</li> </ul>
Executive Team	means the President & CEO (CEO), the Chief Operating Officer (COO), and the Vice Presidents (VPs) of NSBI.
Foreign demand for disclosure	<p>means as defined under Section 2(1)(d) <i>Personal Information International Disclosure Protection Act (PIIDPA)</i>, which states:  “2(1) In this Act,  ...  “(d) “foreign demand for disclosure” means a subpoena, warrant, order, demand or request that is  (i) from a foreign court, an agency of a foreign state or another authority outside Canada, and  (ii) for the unauthorized disclosure of personal information to which this Act applies.”</p>

“Form 1” report	means a written report by the Head, NSBI, to the Nova Scotia Minister of Justice, and in the form specified by the <i>PIIDPA Regulations</i> , notifying the Minister of all of the decisions made by the Head, NSBI in a calendar year under subsection 5(3) <i>PIIDPA</i> to allow storage or access of personal information outside Canada.
Head, NSBI	means as defined in the <i>FOIPOP Act</i> , which for NSBI means the Chair of the Board of Directors of NSBI, or an officer or employee of NSBI to which the Chair has delegated his or her authority under the <i>FOIPOP Act</i> – currently the President & CEO and the Chief Operating Officer (COO) of NSBI.
Information Access and Privacy Services (IAP Services)	means IAP Services Unit, a division of Information, Communications & Technology Shared Services (ICTSS).
Mobile electronic device	means a computer, a cell phone or other transportable electronic machine.
Officer	means an officer of NSBI appointed under the <i>NSBI Act</i> , excluding officers of NSBI who are members of the Board of Directors of NSBI –the non-Director officers of NSBI are the Secretary, the President & CEO (CEO), the Chief Operation Officer (COO), and the Vice Presidents (VP’s) of NSBI.
Personal information	means as defined under Section 3(1)(i) <i>Freedom of Information and Protection of Privacy (FOIPOP) Act</i> , which states: “3(1) <i>In this Act,</i> ... “(i) “personal information” means 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.”*

“Personal information” does not include aggregated information about a group of individuals where there is no reasonable expectation an individual could be identified from the aggregated information.

Privacy breach means an event of unauthorized collection, use, disclosure, access, storage or disposal of personal information in violation of the *FOIPOP Act*, *PIIDPA*, *CASL* or the NSBI Privacy Policy.

Privacy complaint means a complaint, in writing, from an individual that believes his or her personal information, in the custody or under the control of NSBI, has been collected, used, disclosed, accessed, stored or disposed in violation of the *FOIPOP Act*, *PIIDPA*, *CASL* or the NSBI Privacy Policy.

Privacy impact assessment (PIA) means a due diligence process which identifies and assesses potential privacy risks that may occur in the course of NSBI operations.

Privacy procedures means workflow steps, supporting templates and checklists that assist in achieving reasonable security arrangements for the management and protection of personal information.

Program or service means a program or service offered or administered by NSBI and intended to serve clients, prospective clients, employees or the public.

Reasonable security arrangements means the security measures are appropriate to the sensitivity of the personal information and the likelihood and impact of a potential privacy breach.

Record means as defined under Section 3(1)(k) *FOIPOP Act* which states:  
*“3(1) In this Act,  
...  
(k) “record” 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;”*

Record life cycle	means the stages through which NSBI records pass beginning with initial receipt or creation, through active and semi-active use, to authorized disposition whether by transfer to the Public Archives of Nova Scotia or secure destruction.
Significant change to program or service	means a change in the overall purpose or structure of a program or service or the migration of a program or service to an automated electronic system for collection, use or disclosure of personal information.
Service provider	means a person retained under a contract to perform services for NSBI and in the course of performance of services, uses, discloses, manages, stores or accesses personal information in the custody or under the control of NSBI.
Unit Head	means a management position within NSBI responsible for the operations of a business unit.