# Privacy Impact Assessment

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

**What is a Privacy Impact Assessment?**

The *Freedom of Information and Protection of Privacy Act* ("*FOIPOP*") sets out mandatory requirements relating to personal information held by public bodies. *FOIPOP* also requires that public bodies protect the confidentiality of personal information, and the privacy of the individual who is the subject of that information. This includes protecting the information from theft, loss and unauthorized access to, use of, disclosure, copying or disposal of the information.

A privacy impact assessment is a tool to identify risks and mitigation strategies associated with the use of personal information. It is an essential tool for ensuring compliance with the privacy requirements set out in *FOIPOP* and is a building block of a good privacy management program.[1]

**When Should I Complete a Privacy Impact Assessment?**

You should complete a privacy impact assessment ("PIA") for all new systems, projects, programs or activities. PIAs should also be completed when any significant changes are being contemplated to projects, programs or systems. There are a variety of PIA templates available online.[2] This PIA template was created by the Office of the Information and Privacy Commissioner for Nova Scotia and it incorporates elements of a number of existing templates.

## Privacy Impact Assessment

**Notice to Users**

This document is intended to provide general information only. It is not intended nor can it be relied upon as legal advice. As an independent agency mandated to oversee compliance with *FOIPOP, MGA* and *PHIA* the Office of the Information and Privacy Commissioner for Nova Scotia cannot approve in advance any proposal from a public body. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. The contents of this document do not fetter or bind this office with respect to any matter, including any complaint investigation or other matter respecting which the Information and Privacy Commissioner for Nova Scotia[3] will keep an open mind. It remains the responsibility of each public body to ensure that they comply with their responsibilities under the relevant legislation. Visit us at: http://foipop.ns.ca/

---

[1] For more information about Privacy Management Programs visit the website of the Freedom of Information and Protection of Privacy Review Office website at: http://foipop.ns.ca/

[2] See for example the Capital District Health Authority's PIA form at http://www.cdha.nshealth.ca/privacy-confidentiality/documents , the Government of Nova Scotia template at: https://novascotia.ca/just/IAP/_docs/Appendix%20B%20PIA%20Template.pdf , the Government of British Columbia templates and guidance documents at: http://www.cio.gov.bc.ca/cio/priv_leg/foippa/pia/pia_index.page?#DoINeedCompPIA

[3] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act*, and the *Privacy Review Officer Act*.

# Project Name: _____

**Document Version, Review and Approval History**

| Version | Author | Nature of Change | Date |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |

## A. General Information

1. **Name of Program or Service**
2. **Name of Department, Branch and Program Area**
3. **Name of Program or Service Representative**
4. **Contact Information**

## B. Description

1. **Description of the Initiative:** Provide a summary of the program, project activity or system, describe its purposes, goals and objectives. Explain the need for the new program, project or system and its benefits.
2. **Scope of this PIA:** Explain what part or phase of the initiative the PIA covers and what it does not cover.
3. **Elements of Information or Data**: List the personal information data elements involved in the initiative. This could include citizen's name, age, address, educational history, work status, health information, financial information, photos, comments on a blog, license numbers or hiring data.
4. **Description of Information Flow (include text and diagram)**: Attach an information flow diagram showing how information will be collected and disclosed as a result of the initiative. See **Appendix A** for a sample information flow diagram.

If your initiative will not involve the collection, use or disclosure of personal information, you can stop here and submit this document to your privacy officer.

## C. Collection, Use and Disclosure of Personal Information

1. **Limiting Collection, Use and Disclosure:** Privacy is a fundamental right of citizens and so any limitation on the privacy of citizens should be carefully analyzed to ensure such limitation is warranted. If your project involves highly sensitive personal information, a broad collection of personal information or a serious impingement on privacy[4] answer the following four questions before proceeding:

    a. **Is the measure demonstrably necessary to meet a specific need?** At a minimum, the objective must relate to societal concerns which are pressing and substantial in a free and democratic society. To be "demonstrably necessary" the public body should explain the rational connection between the specific need and the project.

    b. **Is it likely to be effective in meeting that need?** Provide empirical evidence to support the initiative.

    c. **Is the loss of privacy proportional to the need?** Explain how the collection, use and/or disclosure of personal information will be undertaken in the least privacy invasive manner possible. Minimizing the number of data elements collected, limiting access to the data and short retention periods are all examples of reducing the privacy invasive impact.

    d. **Is there a less privacy invasive way of achieving the same end?** Explain what other less privacy invasive methods have already been tried to meet the identified need.

Based on this analysis you may decide you do not need to collect, use or disclose personal information for your project. You may decide to reduce the data elements (you need to go back and redo part B before proceeding) or you may determine that you can justify the scope of your collection, use and/or disclosure and so proceed to question 2.

2. **Legal Authority for the Collection, Use and Disclosure of Personal Information:** For each of the collection, use and disclosures identified, evaluate your public body's legal authority and complete the following table. Refer to **Appendix B** for an example of an authorities summary table. Refer to **Appendix C** for a summary of the authorities to collect, use and disclose personal information under *FOIPOP.*

| **Personal Information Authorities Summary** | | | |
|---|---|---|---|
| | **Personal Information Description/Purpose** | **Type** | **FOIPOP Authority** |
| 1. | | | |
| 2. | | | |
| 3. | | | |
| 4. | | | |
| 5. | | | |

[4] Typically projects such as video surveillance, collection or use of GPS data, any covert surveillance, use of biometrics etc. should be considered highly sensitive and will require this preliminary analysis.

3. **Compliance with *Personal Information International Disclosure Protection Act ("PIIDPA")*:**
   *PIIDPA* requires that personal information in the custody or control of a public body shall not be stored or accessed outside of Canada, subject to limited exceptions (s.5(1)). Set out here whether or not there will be any proposed storage or access outside of Canada and if so, describe what *PIIDPA* exceptions apply. See **Appendix D** for a summary of the *PIIDPA* exceptions.

| **Personal Information International Disclosure Protection Act Authorities** | | | |
|---|---|---|---|
| | **Personal Information Description/Purpose** | **Type** | **PIIDPA Authority** |
| 1. | | | |
| 2. | | | |
| 3. | | | |

## D. Correction, Accuracy and Retention of Personal Information

1. **Correction and Accuracy:**
   - **a.** How is an individual's information updated or corrected?
   - **b.** If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated?
   - **c.** If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation? (See s. 25 of *FOIPOP* for further information on correction and accuracy obligations).

2. **Retention:**
   - **a.** Does your initiative use personal information to make decisions that directly affect an individual? If yes, please explain.
   - **b.** Do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual? (See s. 24(4) of *FOIPOP*).

## E. Security of Personal Information

1. **Reasonable security:** *FOIPOP* requires that public bodies protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal of personal information (s. 24(3) *FOIPOP*).
   - **a. Administrative safeguards** – Describe administrative safeguards (such as policies, training, contract provisions, consent forms etc.).
   - **b. Technical Safeguards** – Describe technical safeguards (such as passwords and user ID, authentication, encryption, firewalls and intrusion detection, secure transmission, disaster recovery).
   - **c. Physical Safeguards** – Describe physical safeguards (such as secure access, laptops secured to desk, alarm systems).
   - **d. Auditing** – Describe auditing capability and strategies (audit logs, records of user activity, proactive and focused audit capacity).

If your initiative involves the creation of a new system, consider completing a security threat and risk assessment.

2. **Access Matrix:** Personal information should only be used and disclosed as permitted under *FOIPOP*. Access to personal information must be limited to those employees whose job responsibilities require that they access the personal information. Attach a copy of the user access matrix. A user access matrix will list all of the position types (eg. clerical, manager of investigations, finance director) across one axis and all of the personal information types (or file types or data modules) across the other. The matrix will identify by position which individuals will have access to the identified data. See **Appendix E** for an example of an access matrix.

## F. Risk Mitigation

Assess the impact on privacy, confidentiality and security of personal information as a result of the new program or service or change and make recommendations for mitigation of privacy risks. See **Appendix F** for examples of risks and mitigation strategies.

### Risk Mitigation Table

| | Risk | Mitigation Strategy | Likelihood | Impact |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |

## G. Action Plan

The purpose of this section is to provide an action plan to implement the recommendations listed in section F to reduce the privacy risks that have been identified. This section will provide a mechanism to track the recommendations, as well as describe responses to the recommendations of the PIA. Ensuring the recommended mitigations are implemented according to the action plan is the program area's responsibility, and may be followed-up by the privacy officer at any point.

| Privacy Risk Action Plan | | |
|---|---|---|
| **Mitigation Strategy** | **Steps Required & Responsible Employee** | **Date to be Achieved** |
| | | |
| | | |
| | | |

**PIA Review Date: _____**

PIAs require regular review to ensure that the system, project or program has not substantially changed and to ensure that mitigation strategies have been properly implemented. In addition, changes in other areas (such as technology or the implementation of other related programs) may create new risks that should be identified and mitigated. Typically the review date is selected based on the action plan – within six months of the final required completion dates is a good standard to use.

## H. Approvals

**Completed by:**

[Insert position] Date

**Reviewed by:**

Privacy Officer Date

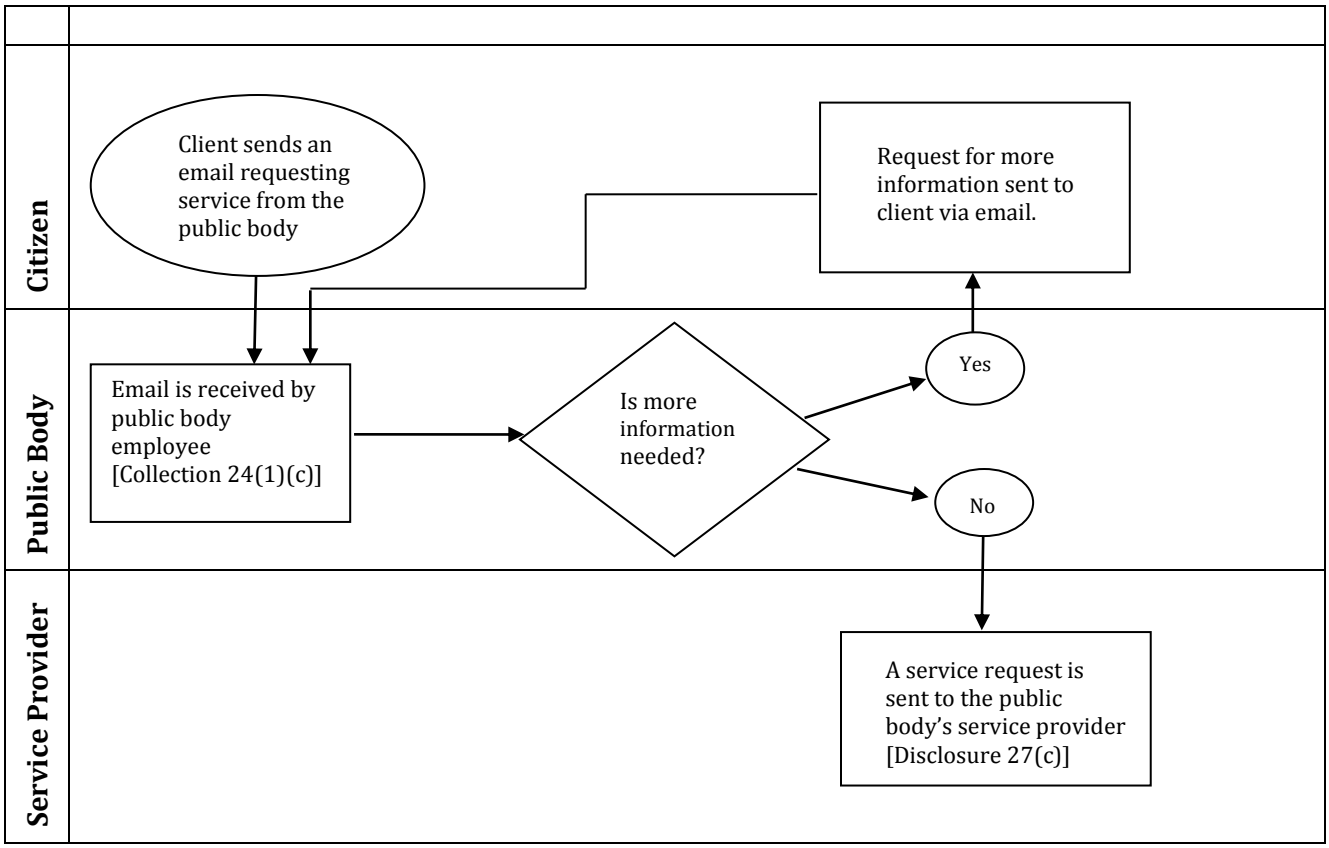
[Insert position] Date

**Approved by:**

[Insert Executive Sponsor] Date

## Appendix A: Sample Information Flow Diagram

***Example:***




## Appendix B: Sample Authorities Summary Table

Using the example given in Appendix A, the table below lists the authorities.

| **Personal Information Authorities Summary** | | | |
|---|---|---|---|
| | **Description/Purpose** | **Type** | **FOIPOP Authority** |
| 1. | *Email received from client requesting service* | *Collection* | *24(1)(c)* |
| 2. | *Service request transferred to service provider contracted by public body* | *Disclosure* | *27(c)* |

## Appendix C: Summary of Authorities Under *FOIPOP*

| | |
|---|---|
| **Collection** | |
| 24(1)(a) | The collection of the information is expressly authorized by or pursuant to an enactment (identify the enactment and section) |
| 24(1)(b) | The information is collected for the purpose of law enforcement (review the definition of law enforcement in s. 3(1)(e) to ensure it applies) |
| 24(1)(c) | The information relates directly to, and is necessary for, an operating program or activity of the public body |
| **Use** | |
| 26(a) | Use is for the purpose for which the information was obtained or compiled, or for a use compatible with that purpose (to determine if a use if compatible review the requirements set out in s. 28) |
| 26(b) | The individual the information is about has identified the information and has consented to the use (such consent should generally be in writing, dated and identifying the information) |
| 26(c) | The use is for a purpose for which the information may be disclosed to the public body pursuant to s. 27 (check the disclosure list below) |
| **Disclosure** | |
| 27(a) | In accordance with this Act or as provided pursuant to another enactment (identify the enactment and section) |
| 27(b) | The individual the information is about has identified the information and consented in writing to its disclosure |
| 27(c) | For the purpose for which it was obtained or compiled, or a use compatible with that purpose (to determine if a disclosure is for a compatible purpose review the requirements set out in s.28) |
| 27(d) | For the purpose of complying with an enactment or with a treaty, arrangement or agreement made pursuant to an enactment (identify the enactment and section and attached the agreement if applicable) |
| 27(e) | For the purpose of complying with a subpoena, warrant, summons or order issued or made by a court, person or body with jurisdiction to compel the production of information |
| 27(f) | To an officer or employee of a public body if the information is necessary for the performance of the duties of, or for the protection of the health or safety of, the officer or employee |
| 27(g) | To a public body to meet the necessary requirements of government operation |
| 27(h) | For the purpose of collecting a debt or fine owing by an individual to the public body or making a payment owing by the public body to an individual |
| 27(i) | To the Auditor General or other prescribed person for audit purposes |
| 27(j) | To a member of the House of Assembly who has been requested by the individual, whom the information is about, to assist in resolving a problem |
| 27(k) | To a representative of the bargaining agent who has been authorized in writing by the employee, whom the information is about, to make an inquiry |
| 27(l) | To the Public Archives of Nova Scotia, or the archives of a public body for archival purposes |
| 27(m) | To a public body or law-enforcement agency in Canada to assist in an investigation undertaken with a view to law enforcement or from which a law-enforcement proceeding is likely to result |
| 27(n) | If the public body is a law-enforcement agency and the information is disclosed to another law-enforcement agency |
| 27(o) | If the head of the public body determines that compelling circumstances exist that affect anyone's health or safety |
| 27(p) | So that the next of kin or a friend of an injured, ill or deceased individual may be contacted |
| 27(q) | For research, archival or historical purposes as provided in sections 29 and 30 |

## Appendix D: Authority to Disclose & Store Personal Information Outside of Canada

***Personal Information International Disclosure Protection Act***

| | | |
|---|---|---|
| **Application of the Act** | | |
| 3<br><br>4 | *PIIDPA* applies to every public body and municipality and to all directors, officers and employees as well as to all employees and associates of a service provider.<br>*PIIDPA* does not apply to records listed in s. 4 which include:<br>• Published material or material that is available for purchase by the public<br>• Material that is a matter of public record | |
| **Access and Storage Outside Canada - Authorities** | | |
| 5(1) | **Rule** | A public body shall ensure that personal information is stored and accessed only in Canada unless authorized under *PIIDPA* |
| 5(1)(a) | **Consent** | The individual the information is about has identified the information and has consented, in the manner prescribed by regulation, to it being stored in or accessed from outside Canada. |
| 5(1)(b) | **PIIDPA Disclosure** | The information is stored or accessed outside of Canada for the purpose of disclosure allowed under *PIIDPA* (see list below) |
| 5(1)(c) | **Permission** | The head of the public body has allowed storage outside of Canada pursuant to s. 5(2):<br>• If the head considers the storage or access is to meet the necessary requirements of the public body's operation, (subject to any restrictions or conditions the head considers advisable)<br>• The head must report the access or storage decision to the Minister within the timeline set out in the Act (s. 5(3)) |
| **Disclosure Outside Canada - Authorities** | | |
| 9(2)(b) | **Consent** | The individual the information is about has identified the information and consented, in writing, to its disclosure inside or outside Canada |
| 9(2)(c) | **Enactment** | In accordance with an enactment of the Province, the Government of Canada or the Parliament of Canada that authorizes or requires its disclosure |
| 9(2)(d) | **Agreement** | In accordance with a provision of a treaty, arrangement or agreement that authorizes or requires its disclosure and is made under an enactment of the Province, the Government of Canada or the Parliament of Canada |
| 9(2)(e) | **To head** | To the head of the public body, if the information is immediately necessary for the performance of the duties of the head |
| 9(2)(f) | **To employee** | To an employee of the public body and the information is immediately necessary for the protection of the health or safety of the employee |
| 9(2)(g) | **To legal counsel** | To legal counsel for the public body, for use in civil proceedings involving the Government of the Province or the public body |
| 9(2)(h) | **Debts** | To collect moneys owing by an individual to the Province or public body or for making a payment owing by the Province or public body |
| 9(2)(i) | **Motor vehicle** | For the purpose of licensing or registration of motor vehicles or drivers or verification of motor vehicle insurance, registration or drivers' licenses |
| 9(2)(j) | **Compelling circumstances** | Where the head of the public body determines that compelling circumstances exist that affect anyone's health or safety |
| 9(2)(k) | **Next of kin** | So next of kin or friend of injured or deceased individual may be contacted |
| 9(2)(l) | **Research Archives** | For research purposes in accordance with s. 10<br>To a provincial or public body archive in accordance with s. 11 |
| 9(3) | **Law enforcement** | A public body that is a law enforcement agency may disclose to another law enforcement agency in Canada or in a foreign country under an agreement or enactment of Canada or the province |
| 9(4) | **Temporary** | The head of a public body may allow an employee to transport personal information outside Canada temporarily if the head considers it is necessary for the performance of the duties of the employee to transport the information in a computer, cell phone or other mobile device. |

## Appendix E: Sample Access Matrix

The following example is for a database intended to manage landlord and tenant complaint information. Access to personal information must be strictly limited to those needing the information to carry out their job duties. Depending on how duties are assigned, it may be the clerk's responsibility to input the initial information identifying the landlord, tenant and the complaint summary. If this is not true, then limit the clerk's access to those data elements required.

The Deputy Minister would not typically have access to a database of this nature and so has not been assigned any access rights in the matrix below. The matrix assumes that the landlord and tenant identity information is not contained in the complaint summary nor in the enforcement outcome. The investigation notes could, of course, contain a variety of information including personally identifiable information of the landlord and tenant.

| | **Landlord Information**[5] | **Tenant Information** | **Complaint Summary** | **Investigation Notes** | **Enforcement Outcome** |
|---|---|---|---|---|---|
| **Clerical** | ✓ | ✓ | ✓ | | ✓ |
| **Program Director** | ✓ | ✓ | ✓ | | ✓ |
| **Manager of Investigations** | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Investigator** | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Deputy Minister** | | | | | |

[5] Identification information would include name, address and other contact information. This module may be common across a variety of databases.

**Appendix F: Sample Risks and Mitigation Strategies**

You will need to adopt a scale to measure likelihood and impact. High, medium and low will do or you can choose a numerical scale for greater subtlety in choice.

| | Risk | Mitigation Strategy | Likelihood | Impact |
|---|---|---|---|---|
| 1 | Authorized user views record for personal reasons | • Log all read only and change activity<br>• Monitor logs regularly, conduct spot audits and ensure audit capacity in response to complaints<br>• Oath of employment and confidentiality agreements<br>• Training | Likelihood increases with more users | • More sensitive data results in higher impact<br>• More data exposed by incident results in higher impact |
| 2 | Service provider fails to report privacy breach to public body | Contractual terms:<br>• Require reporting within 24 hours<br>• Impose penalties for failure to report and late reporting<br>• Require the service provider to log all read only and change activity and to monitor the logs regularly<br>• Permit the public body to conduct audits and to review service provider audit logs | • Experience with the service provider may help determine this<br>• Severity of consequences for service provider may lower the likelihood | Same considerations as above |
| 3 | Client's personal information is compromised when transferred to the service provider | Transmission is encrypted and over a secure line | Low – depending on the quality of the encryption | Same considerations as above |