**Office of the Information and Privacy Commissioner for Nova Scotia**

# Privacy Management Program – Gap Analysis

## For Larger Public Bodies and Municipalities

***Freedom of Information and Protection of Privacy Act* and *Municipal Government Act Part XX***

**Introduction:**

This document was developed by the Information and Privacy Commissioner for Nova Scotia[1] and is intended to assist larger public bodies and municipalities with developing and implementing a robust privacy management program. An overview of the elements of a robust privacy management program is contained in *Privacy Management Program At-a-Glance* on the Office of the Information and Privacy Commissioner for Nova Scotia's website at: http://foipop.ns.ca/ . This Gap Analysis document provides detailed information about each of the elements of a privacy management program. The goal of the Gap Analysis is to identify shortcomings in the program. The Gap Analysis results should then be used to develop a privacy oversight and review plan that addresses each of the identified gaps.

We have developed privacy management program tools and gap analysis worksheets for health custodians and smaller municipalities. Check the Tools & Guidance section of our website for these materials.

**Contact Us:**

If you have questions or comments with respect to this document please contact us at:

Office of the Information and Privacy Commissioner for Nova Scotia
PO Box 181
Halifax, NS B3J 2M4
Phone: 902-424-4684 Toll Free: 1-866-243-1564

[1] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the 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*.

**Instructions:**

This gap analysis tool begins with a Gap Analysis Summary document (page 3). When complete this will serve as a one page summary of your review results. Your goal is to develop a visual gap analysis by assigning red, yellow or green to the outcome of your assessment for each of the elements of your privacy management program ("PMP").

**Step 1:** Begin by assessing the two categories of building blocks: organizational commitment and program controls. Within each category are a series of requirements. For each requirement we have provided a list of essential elements. So, for example the Organizational Commitment requirement for buy-in from the top lists three requirements from senior management (see page 4). Record your evaluation of each element by describing the current state of affairs in your organization. Be as honest and critical as you can. The goal here is to accurately state your organization's current status.

**Step 2:** For each requirement score your organizations compliance on a scale of 1 to 3. Feel free to give partial points. Ratings are explained below.

**Step 3:** Average the score for the elements of each requirement to come up with an overall score that you will record in the overall rating row.

**Step 4:** Record the overall score then assign a colour to it and record the colour on the summary sheet at page 3. Colour ratings are explained below.

**Step 5:** Once you have completed all of your ratings, review the summary sheet at page 3 and develop a plan to move all of your ratings to green (a privacy oversight and review plan).

| **Sample – Gap Analysis Summary** | |
|---|---|
| **PMP Requirement** | **Overall Gap Analysis Rating** |
| **Building Blocks – Organizational Commitment** | |
| a. Buy-in from the Top | 1.9 |
| b. Privacy Officer | 2.2 |
| c. Privacy Office | 2.6 |
| d. Reporting | 2.7 |
| **Building Blocks – Program Controls** | |
| a. Personal Information Inventory | 1.3 |
| b. Policies | 1.8 |
| c. Risk Assessment Tools | 2.1 |
| d. Training and Education Requirements | 2.0 |
| e. Breach and Incident Management Protocols | 2.7 |
| f. Service Provider Management | 1.4 |
| g. External Communication | 1.5 |
| **Ongoing Assessment and Revision – Oversight and Review Plan** | |
| a. Develop Oversight and Review Plan | 2.0 |
| **Ongoing Assessment and Revision – Program Controls** | |
| a. General Requirements | 2.2 |
| b. Update Personal Information Inventory | 1.6 |
| c. Revise Policies | 2.5 |
| d. Treat Risk Assessment Tools as Evergreen | 1.9 |
| e. Modify Training and Education | 2.8 |
| f. Adapt Breach and Incident Response Protocols | 2.2 |
| g. Fine-tune Service Provider Management | 2.1 |
| h. Improve External Communication | 1.7 |

| Gap Analysis Summary | |
|---|---|
| **PMP Requirement** | **Overall Gap Analysis Rating** |
| **Building Blocks – Organizational Commitment** | |
| a. Buy-in from the Top | |
| b. Privacy Officer | |
| c. Privacy Office | |
| d. Reporting | |
| **Building Blocks – Program Controls** | |
| a. Personal Information Inventory | |
| b. Policies | |
| c. Risk Assessment Tools | |
| d. Training and Education Requirements | |
| e. Breach and Incident Management Protocols | |
| f. Service Provider Management | |
| g. External Communication | |
| **Ongoing Assessment and Revision – Oversight and Review Plan** | |
| a. Develop Oversight and Review Plan | |
| **Ongoing Assessment and Revision – Program Controls** | |
| a. General Requirements | |
| b. Update Personal Information Inventory | |
| c. Revise Policies | |
| d. Treat Risk Assessment Tools as Evergreen | |
| e. Modify Training and Education | |
| f. Adapt Breach and Incident Response Protocols | |
| g. Fine-tune Service Provider Management | |
| h. Improve External Communication | |

**Gap Analysis Ratings & Colour Ratings for Summary Chart**

| Rating | Colour Code | Rating Description |
|---|---|---|
| 1.0 – 1.9 | Red | Little to no evidence of compliance - documented or in practice. |
| 2.0 – 2.5 | Yellow | No documented evidence of compliance but some evidence of effective practice in compliance or documented practice requirement with only limited evidence of implementation. |
| 2.6 – 3.0 | Green | Documented and substantial practical compliance. |



| Building Blocks – Organizational Commitment | | |
|---|---|---|
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **a. Buy-in from the Top** | **Overall Rating** | |
| 1. Senior management endorses the program controls (policies, risk assessments, training). | | |
| 2. Senior management provides resources that the privacy management program needs to succeed. | | |
| 3. Senior management monitors program and reports to board of directors as appropriate. | | |
| **b. Privacy Officer** | **Overall Rating** | |
| 4. A senior manager (Director or above) is assigned responsibility for overseeing the organization's compliance. | | |
| **c. Privacy Office** | **Overall Rating** | |
| 5. Privacy Officer is supported by dedicated staff. | | |
| 6. Role of the privacy office is defined. | | |
| 7. Staff have delegated responsibilities to monitor compliance. | | |
| 8. Staff foster culture of privacy within the organization. | | |
| 9. Staff work to ensure that privacy protection is built into every major function involving the use of personal information including policies, programs, contracts, legislation, regulations, IT systems, communication, etc. | | |
| **d. Reporting** | **Overall Rating** | |
| 10. There are privacy reporting mechanisms that ensure that the right people know how the privacy management program is structured and whether it is functioning as expected. | | |



| Building Blocks – Organizational Commitment continued | | |
|---|---|---|
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **d. Reporting continued** | | |
| 11. Senior Management receive regular reports on privacy and compliance. | | |
| 12. Reporting mechanisms are reflected in the organization's program controls. | | |
| 13. An internal audit and assurance program monitors compliance with privacy policies. | | |
| 14. An escalation procedure has been clearly defined and explained to all employees for security breach or when a customer complains. | | |
| 15. The escalation procedure is monitored to ensure necessary steps are being taken when triggered. | | |
| 16. The reporting program has documented reporting structures. | | |
| **Building Blocks – Program Controls** | | |
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **a. Personal Information Inventory** | **Overall Rating** | |
| 1. The organization has completed a personal information inventory or equivalent. | | |
| 2. The organization is able to identify: | | |
| (i) The type of personal information that it holds. | | |
| (ii) Where the personal information is held. | | |
| (iii) Why/how it is collecting personal information. | | |
| (iv) Uses of personal information. | | |
| (v) Why/to whom it is disclosing personal information. | | |
| (vi) The sensitivity and/or classification of personal information. | | |

| Building Blocks – Program Controls continued | | |
|---|---|---|
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **b. Policies** | **Overall Rating** | |
| 3. Five key policies are in place:<br>(i) Collection, use, disclosure of personal information including requirements for consent and notification | | |
| (ii) Access to and correction of personal information. | | |
| (iii) Retention and disposal of personal information. | | |
| (iv) Responsible use of information and information technology including administrative, physical and technological security controls and appropriate access controls. | | |
| (v) Challenging compliance. | | |
| **c. Risk Assessment Tools** | **Overall Rating** | |
| 4. Privacy risk assessments are required throughout the organization for all new projects involving personal information and on any new collection use or disclosure of personal information. | | |
| 5. A process has been developed for identifying and mitigating privacy and security risks including the use of privacy impact assessments and security threat risk assessments. | | |



| Building Blocks – Program Controls continued | | |
|---|---|---|
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **c. Risk Assessment Tools continued** | | |
| 6. Procedures have been developed for conducting such assessments and a review and approval process has been developed that involves the privacy office when designing new initiatives, services or programs. | | |
| **d. Training and Education Requirements** | **Overall Rating** | |
| 7. All employees require general privacy protection training. | | |
| 8. Privacy training is mandatory for all new employees. | | |
| 9. Training processes are documented and participation and success are measured. | | |
| 10. Individuals who handle personal information directly receive additional training specifically tailored to their roles. | | |
| 11. Training and education are recurrent and the content of the program is periodically revisited and updated to reflect changes. | | |
| **e. Breach and Incident Management Response Protocols** | **Overall Rating** | |
| 12. There is a procedure for the management of personal information breaches. | | |
| 13. There is a person responsible for managing a breach. | | |
| 14. Responsibilities for internal and external reporting of the breach are defined. | | |

| Building Blocks – Program Controls continued | | |
|---|---|---|
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **f. Service Provider Management** | **Overall Rating** | |
| 15. Contractual or other means are in place to protect personal information. | | |
| 16. Transborder data flows and requirements of the foreign regime are addressed in service provider arrangements. | | |
| 17. Sensitivity of personal information is addressed in service provider arrangements. | | |
| 18. Privacy requirements for service providers include:<br>(i) Compliance requirement such as binding the service provider to the policies and practices of the organization and requiring breach notification. | | |
| (ii) Training and education for all service provider employees with access to personal information. | | |
| (iii)Restrictions on sub-contracting. | | |
| (iv)Audits. | | |
| (v) Agreements with service provider employees stating that they will comply with the organization's privacy policies and protocols. | | |
| **g. External Communication** | **Overall Rating** | |
| 19. There is a procedure for informing individuals of their privacy rights. | | |
| 20. There is a procedure for informing individuals of the program controls. | | |

| Building Blocks – Program Controls continued | | |
|---|---|---|
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **g. External Communication continued** | | |
| 21. The external communication is clear and understandable and not simply a reiteration of the law. | | |
| 22. External communication:<br>(i) Provides enough info so that individuals know the purpose of the collection, use and disclosure of personal information and how it is safeguarded and how long it is retained. | | |
| (ii) Notifies individuals if their personal information is being transferred outside of Canada. | | |
| (iii) Includes information on who to contact with questions or concerns about the management of personal information. | | |
| (iv) Is easily available to individuals. | | |
| (v) Individuals are aware of how to access & correct their personal information. | | |
| (vi) Individuals are aware of how to complain including the right to submit a complaint to the Information and Privacy Commissioner for Nova Scotia. | | |

| Ongoing Assessment and Revision (Privacy Brand Management)<br>Oversight and Review Plan | | |
|---|---|---|
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **a. Develop Oversight and Review Plan** | **Overall Rating** | |
| 1. The Privacy Officer develops an oversight and review plan on an annual basis that sets out how the privacy management program's effectiveness will be monitored and assessed. | | |
| 2. The plan establishes performance measures. | | |
| 3. The plan includes a schedule of when all policies and other program controls will be reviewed. | | |
| **Assess & Revise Program Controls** | | |
| **a. General Requirements** | **Overall Rating** | |
| 1. The effectiveness of program controls are monitored periodically, audited and revised where necessary. | | |
| 2. The monitoring addresses the following:<br>(i) The latest threats and risks. | | |
| (ii) Whether program controls are addressing new threats. | | |
| (iii) Whether program controls are reflecting the latest compliance audit findings or guidance of the privacy commissioners. | | |
| (iv) Whether new services being offered involve increased collection, use or disclosure of personal information. | | |
| (v) Whether training is occurring and if it is effective. | | |
| (vi) Whether policies and procedures are being followed. | | |
| (vii) Whether the privacy management program is up to date. | | |



| Assess & Revise Program Controls continued | | |
|---|---|---|
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **a. General Requirements continued** | | |
| 3. Problems identified during monitoring are documented and addressed. | | |
| 4. The Privacy Officer conducts periodic assessments to ensure key processes are being respected. | | |
| 5. The organization has developed metrics to gauge progress with respect to compliance. | | |
| 6. Assessments of program controls are conducted in a focused, continuous and thorough manner. | | |
| **b. Update Personal Information Inventory** | **Overall Rating** | |
| 7. The personal information inventory is kept current. | | |
| 8. New collections of personal information are identified and evaluated. | | |
| 9. New uses of personal information are identified and evaluated. | | |
| **c. Revise Policies** | **Overall Rating** | |
| 10. Policies are reviewed and revised as needed, following assessments or audits, in response to a breach or complaint, new guidance, industry-based best practices or as a result of environmental scans. | | |
| **d. Treat Risk Assessment Tools as Evergreen** | **Overall Rating** | |
| 11. Privacy impact assessments are treated as evergreen documents so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed. | | |

| Assess & Revise Program Controls continued | | |
|---|---|---|
| **List of Expectations** | **Evidence of Compliance** | **Gap Rating** |
| **d. Treat Risk Assessment Tools as Evergreen continued** | | |
| 12. Security threat and risk assessments are treated as evergreen documents so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed. | | |
| **e. Modify Training and Education** | **Overall Rating** | |
| 13. Training and education programs are reviewed and modified on a periodic basis as a result of ongoing assessments. | | |
| 14. Changes to program controls are effectively communicated to employees as they are made, or in "refreshed" education and training modules. | | |
| **f. Adapt Breach and Incident Response Protocols** | **Overall Rating** | |
| 15. Breach and incident management response protocols are reviewed and revised to implement best practices or recommendations. | | |
| 16. The breach and incident response protocol is reviewed and revised to implement lessons learned from post-incident reviews. | | |
| **g. Fine-tune Service Provider Management** | **Overall Rating** | |
| 17. Contracts with service providers are reviewed and, where necessary, fine-tuned. | | |
| **h. Improve External Communication** | **Overall Rating** | |
| 18. External communications explaining privacy policies are reviewed, updated and clarified as needed. | | |