Accountable Privacy Management in BC's Public Sector
Contents

Accountable Privacy Management In BC's Public Sector 2

INTRODUCTION 3

What is accountability? 4
Steps to setting up the program 4

A. PRIVACY MANAGEMENT PROGRAM ESSENTIALS 5

1. Demonstrating Commitment to Privacy Compliance 5
   Demonstrating senior management commitment and support 5
   Designate and empower a Privacy Officer 6
   Compliance reporting 7

2. Program Controls 8
   Personal information inventory 8
   Compliance policies 9
   Risk assessment tools 12
   Training 13
   Breach and incident management response protocols 13
   Service provider management 14
   Communicating with individuals and demonstrating accountability 15

B. ONGOING ASSESSMENT AND REVISION 16

1. Develop an Oversight and Review Plan 16
2. Assess and Revise Program Controls 16

Conclusion 17

PRIVACY MANAGEMENT PROGRAM – AT A GLANCE 18

A. Building Blocks 18
B. Ongoing Assessment and Revision 19

APPENDIX A 20
This document provides step-by-step guidance for British Columbia public bodies on how to implement effective privacy management programs.

A privacy management program ensures that privacy is built into all initiatives, programs or services by design. Responsible management of personal information is critical to build and maintain the trust of citizens, who are increasingly concerned about the effect of new and emerging technologies on personal privacy, especially digital solutions for managing personal information. And, an investment in privacy protection today can help prevent a costly data breach tomorrow.

As the volume, type and sensitivity of personal data in the custody or control of a public body will vary, privacy management programs must be adapted to the unique needs of the public body. This document provides a scalable framework all public bodies can use.

The Office of the Information and Privacy Commissioner for BC (“OIPC”) intends to use this document in its enforcement work and will be looking for evidence of a privacy management program in future investigations and audits.
As public bodies seek to serve British Columbians in innovative ways, many are looking for efficiencies in how they design and deliver services, and for new approaches to old problems. Analyzing personal information is an increasingly critical part of these efforts. It is also key to public bodies gaining a better understanding of citizens' needs. More and more of this information is electronic personal information, and many of the analytic technologies used in the private sector are also being adopted in the public sector.

Public bodies have the power to compel citizens to give up their personal information in ways that businesses cannot. Individuals have a choice to share personal information with businesses in ways that they do not with government. Public bodies, therefore, have a legal and moral obligation to responsibly manage personal information.

This is the context, and reason, for this document, which aims to guide British Columbia’s public bodies on what it means to be accountable for privacy and what the OIPC expects to see in a privacy management program. Public bodies need to design and implement practical, effective and properly-resourced privacy management programs that are consistent with the principles outlined in this document, as well as with the provisions of the Freedom of Information and Protection of Privacy Act ("FIPPA").

The first part of this document outlines the fundamentals of a privacy management program, including an organizational commitment to privacy compliance, program controls, risk assessment and training. The second part of the document outlines how public bodies should review, revise and maintain their privacy management programs on an ongoing basis.¹

Like all management tools, privacy management programs have to be kept current. They should remain practical and effective in the face of changing services, administrative structures and all applicable legislation. A public body cannot take a snapshot approach; creating a privacy management policy and then leaving it on the shelf. Privacy management should become part of an organization’s routine operational tasks.

This document does not provide legal or other advice. It does not affect the powers, duties or functions of the Information and Privacy Commissioner or the rest of the OIPC respecting any complaint, investigation or other matter under or connected with FIPPA and the matters addressed in this document, respecting which the Commissioner and OIPC retain an open mind.

¹ The appendix to this document offers links to privacy compliance resources, including resources from the OIPC and other regulators, dealing with different aspects of privacy compliance. These may be of further assistance to public bodies in designing and implementing their privacy management programs.
What is accountability?

Accountability in relation to privacy means accepting responsibility for personal information protection. In order to demonstrate accountability for privacy, a public body must have comprehensive policies, procedures and practices in place that comply with applicable privacy laws. These practices, taken as a whole, constitute a privacy management program.

While the concept of accountability may appear to be straightforward, constructing a privacy management program requires thoughtful planning. Employees should be aware of and understand how the program applies. The public should have access to meaningful information about the public body’s privacy management program. And public bodies must be prepared to provide evidence of privacy management to regulators in the wake of an investigation, audit or privacy breach.

Steps to setting up the program

Prior to designing a privacy management program that best meets its needs, a public body should first assess its existing approaches to privacy compliance. To do this, they should consider following these steps to assess their current privacy compliance regime:

1. Appoint a project lead with sufficient privacy knowledge and authority to manage the project and assess the findings (this could be the Privacy Officer, discussed below);
2. Ensure oversight by executive management through a project lead;
3. To the extent necessary, involve human resources, risk management, internal audit and IT personnel;
4. If necessary, obtain outside privacy expertise;
5. Obtain and document information to assess compliance, including thorough staff interviews, file reviews and IT system reviews;
6. Regularly report to executive on progress and implement any resulting direction from executive;
7. Report to executive on any identifiable risk and compliance issues;
8. Provide a final report of all findings to executive with a full mapping of findings against FIPPA’s requirements; and
9. Any other steps that might, in light of the public body’s own situation, be desirable to document its current state of compliance and the way forward.

---

2 Some public bodies may be subject to other legislated privacy requirements e.g., relating to personal health information.
3 These factors are consistent with the AICA/CICA Privacy Maturity Model (March 2011), found at: http://www.cica.ca/resources-and-member-benefits/privacy-resources-for-firms-and-organizations/docs/item48094.pdf.
This section describes the fundamental privacy management building blocks that every public body should have. It is not possible, of course, to describe a universally-applicable approach. For one thing, public bodies vary in size, mandate and functions, and the kinds of personal information they collect, and what they do with it, vary widely. The guidance is intended to be scalable to fit the unique needs of public bodies who work through these building blocks.

Accountability has a number of important elements. FIPPA requires that each public body have a ‘head’, and that the head is explicitly accountable for a number of the privacy obligations in Part 3 of FIPPA. The head has overall responsibility for directing the development, implementation and maintenance of the public body’s privacy protection program, and may delegate this responsibility as appropriate. Especially in larger public bodies, the bottom line is that the head must ensure that a person or persons are responsible for FIPPA compliance within the organization on a day-to-day basis.

Public bodies must be prepared to provide evidence of privacy management to regulators in the wake of an investigation, audit or privacy breach.

**1. Demonstrating Commitment to Privacy Compliance**

The first building block is the development of a robust and well-thought-out internal governance structure that prioritizes privacy compliance and fosters a privacy-respectful culture. This recognizes that more is needed than program controls that give effect to FIPPA’s requirements and underlying privacy principles. In other words, while a public body needs a governance structure and processes that help ensure FIPPA compliance, it needs to go further. Structures and processes are key components, but public bodies need to create and maintain a culture of privacy awareness. This is of fundamental importance to their ability to meet privacy challenges as they arise. It is also a key component of the accountability contemplated by FIPPA.

**a) Demonstrating senior management commitment and support**

Executive-level support is at the heart, therefore, of a privacy-respectful culture and of any successful privacy management program. Executive commitment to FIPPA compliance and to good practices increases the likelihood that the public body’s compliance program will succeed. Executive commitment also fosters the desired privacy culture.

To actively champion a privacy management program, the executive should ensure that all resources necessary to develop, implement, monitor and adapt the program are available to the head. Public bodies face competing demands for public resources, which can be scarce. However, compliance with provincial privacy law is not discretionary; adequate funding and support needs to be devoted to privacy compliance.

In addition to the formal legal sanctions that can flow from non-compliance, proper funding is also necessary to meet public expectations around privacy. Maintaining public trust and
confidence in government’s privacy practices is critically important; the legislative privilege of being able to compel citizens to surrender their personal information depends on that trust and confidence.

**b) Designate and empower a Privacy Officer**

The head or his/her delegate i.e., the Privacy Officer, is responsible for ensuring the public body’s compliance with FIPPA generally, and is responsible for management and direction of the privacy management program. It does not matter whether the Privacy Officer is an executive level manager of a provincial government ministry or the administrator of a small local government—someone must be designated to be responsible for the public body’s privacy compliance and practices.

Of course, others within the public body will have a role in privacy compliance. Day-to-day operations require employees to deal with personal information as part of their duties. These employees clearly have an important role to play in compliance, while the Privacy Officer remains accountable for designing and managing the program.

The Privacy Officer will play many privacy-related roles, including:

- establishing and implementing program controls;
- ongoing assessment and revision of program controls;
- creating all privacy policies and procedures;
- designing and implementing employee training and education;
- monitoring and auditing, with documentation, implementation of the privacy management program;
- representing the public body in the event of an OIPC investigation; and
- demonstrating leadership within the public body in creating and maintaining the desired culture of privacy.

Adequacy of resources is important. In a smaller public body, the Privacy Officer will likely be able to assume other duties without affecting their ability to discharge her or his privacy compliance duties. In larger public bodies, such as a ministry, it is much more likely that the Privacy Officer will not be able to perform other duties without negatively affecting privacy compliance. Similarly, in larger public bodies, it is likely that the Privacy Officer will need staff support. In a ministry that handles a lot of personal information, for example, it is much more likely that the Privacy Officer will be a full-time employee and will need additional staff.

It is important, therefore, for each public body to assess the resources needed to ensure legislative compliance and good practice. This can be done as part of the initial assessment and design of the privacy management program, with appropriate resources and staff being dedicated to carrying it out once the program is approved for implementation.

---

1 Further, when a public body designates someone as its Privacy Officer, it has to ensure that delegations of the duties and functions of the head under FIPPA are validly effected. Pursuant to s. 77 of FIPPA, at the local government level, this involves the passage of resolutions of council or the board, for example. At the provincial level, written delegations are required.

2 Public bodies must keep in mind that designation of a Privacy Officer does not diminish their ultimate accountability for compliance with FIPPA.
Annual budgets should reflect shifting needs for compliance resources, including those driven by changes to legislation; public body administration and management; and new programs involving personal information and outsourcing of services.

c) Compliance reporting

A privacy management program’s controls need to include several types of reporting mechanisms. The goal should be to ensure that the Privacy Officer and executive management are informed, on a regular basis, whether the program is functioning as expected, how and why it is not, and of the proposed fixes.

A key component of compliance reporting is an internal audit program that evaluates and reports on compliance. Audit and assurance processes should include employee interviews and file reviews, both of which should evaluate compliance with objective criteria. External audits may be warranted in some cases, notably where a larger public body has suffered a significant privacy breach. In such cases, the public body should consider retaining a qualified third party to perform the audit or review. Regardless of whether they are routine or triggered by a breach, internal and third-party audit reports may help establish due diligence in response to an investigation or audit by the OIPC.

Another key kind of reporting relates to security breaches or citizen complaints that are reported to the Privacy Officer, who may request assistance from executive management as required. Escalation includes involving those who have responsibility and control over the matter and its solution. This is likely to include, in a larger public body, certainly, IT professionals, security experts, information managers, legal advisers and communication advisers.

A privacy management program must clearly define when and how a matter is to be escalated, and to whom. FIPPA requires that the head of the public body be informed of an unauthorized disclosure of personal information. In instances of other privacy complaints, progress reports about the handling of a matter should also be reported to the Privacy Officer or his or her delegate. This is necessary to ensure that procedures are being followed and required steps are being taken. It may be useful to evaluate the robustness of the escalation and reporting process by conducting a test run of, especially, privacy breach identification, escalation and containment protocols.

Further guidance on documentation and reporting mechanisms is found in Part B (Ongoing assessment and revision).

---

3 See s. 30.5 of FIPPA.
Program controls help ensure that FIPPA's requirements, and the public body's internal governance mechanisms, are implemented throughout the public body.

a) Personal information inventory

A thorough personal information inventory is a fundamental and critically important aspect of privacy compliance. If a public body does not know, to a reasonable degree of specificity, the nature and amount of personal information it is collecting, using, disclosing and retaining, and the purposes and conditions for those activities, it can hardly hope to comply with FIPPA. Creation and maintenance of a personal information inventory is a good example of why public bodies need to document their activities—accountability is at the core of FIPPA and adequate documentation is essential to achieving, and demonstrating, accountability for privacy protection.

This is more than a matter of good practice. A proper personal information inventory is indispensable for compliance with significant FIPPA transparency requirements around personal information holdings.

To begin with, public bodies will need to ensure that their inventory covers only personal information as FIPPA defines it. The term is defined as "recorded information about an identifiable individual other than contact information." If a public body is not sure whether it is collecting "information about an identifiable individual", it should keep in mind that decisions under FIPPA have interpreted the definition in a remedial and liberal way, consistent with modern principles of statutory interpretation and the Supreme Court of Canada. Generally speaking, if information either identifies an individual (including through a unique identifier) or the information could, when combined with other available information, reasonably identify an individual, it will be personal information. In cases of doubt, the public body should seek expert advice on the issue.

Where government ministries have personal information in their custody or control, FIPPA requires the minister responsible for that Act to maintain and publish a personal information directory. The directory must provide, on a ministry-by-ministry basis, information about records of personal information in the custody or control of each ministry. The directory must also include information about the use of those records by each ministry. Further requirements exist, including the requirement for the directory to include information about the information-sharing agreements of each ministry and about PIAs of each ministry.

Further, public bodies other than ministries also have obligations to publish information about their personal information holdings and uses. Their directories must describe the kind of personal information they hold, the categories of individuals whose information they hold, the authority and purposes for collection and categories of persons to whom the information is disclosed or who use it.

---

4 The term ‘contact information’ is defined, essentially, as information to enable someone to contact an individual at a place of business, such as business address, business telephone, and so on.
5 The Interpretation Act mandates a “fair…large and liberal” interpretation of statutes. For discussion of the meaning of ‘personal information’, see, for example, Order F13-04, [2013] B.C.I.P.C.D. No. 4, a case involving GPS monitoring information.
6 FIPPA, ss. 69(2) and (3).
7 FIPPA, s. 69(6).
Regardless of which set of requirements applies, it is difficult to see how a public body can meet these statutory requirements unless it knows what personal information it collects, how it uses it, to whom it is disclosed, for what purposes, and so on. These FIPPA requirements, therefore, give a strong incentive for public bodies to complete and maintain an accurate and comprehensive personal information inventory. In any case, such an inventory is necessary in order to assess existing compliance with FIPPA’s rules overall. It is also necessary in order to design and implement an effective privacy management program. In other words, every aspect of a sound and effective privacy management program begins with this inventory.

Every public body must determine the following factors and document them in an organized, reasonably-detailed, inventory:

- the amount and categories of personal information it holds;
- the number and categories of individuals whose personal information it holds;
- location where personal information is held, both within the public body and where it is held by third parties (including service providers);
- purposes for which personal information is collected, used and disclosed; and
- sensitivity of the personal information the public body holds.8

b) Compliance policies

As discussed earlier, public bodies should, in order to keep the public’s trust, take all reasonable steps to ensure, and be able to demonstrate, FIPPA compliance and good practices. This is also important because, without written policies and procedures, a public body’s FIPPA compliance will be ad hoc and potentially haphazard.

Here are some key privacy issues that public bodies should address through policies:

i. Authority for collection, use and disclosure of personal information;
ii. Requirements for consent and notification;9
iii. Accuracy of personal information;
iv. Individual access to and correction of personal information;
v. Retention and disposal of personal information;
vi. Responsible use of information and information technology, including administrative, physical and technological security controls and appropriate access controls; and
vii. A process for handling privacy-related complaints.

---

8 Further guidance on the elements of a personal information inventory can be found in, among other sources, Securing Personal Information: A Self-Assessment Tool for Organizations, found at http://www.oipc.bc.ca/guidance-documents/1439.

9 For provincial government ministries, but also some other public bodies, policies will also be required for information-sharing and data-linking initiatives, as well as common programs or activities involving the sharing of personal information between two or more public bodies or organizations.
Consideration should also be given to how other public body policies could account for privacy compliance. Policies in relation to contract management, procurement policies, human resources and the disclosure of personal information to regulatory bodies, law enforcement agencies and internal security departments may, for example, need to be drafted or revised.

The next section discusses each of the above key policies in more detail.

i. **Authority for collection, use and disclosure of personal information**
   A key policy component will be guidance for employees on personal information the public body is authorized to collect and for what purposes as well as what use and disclosure of personal information is authorized under FIPPA. This policy should also address when and how the public body may collect personal information indirectly, i.e., other than from the individual whose information is collected. Employees need to understand the FIPPA obligations in this area.

   Policies should address all aspects of the management of personal information and related privacy obligations, including those obligations that are particular to data-linking initiatives, common or integrated programs or activities, and disclosure for research.

ii. **Requirements for consent and notification**
   In certain circumstances, FIPPA requires public bodies to obtain the consent of individuals before collecting their personal information. In other circumstances, individuals must be notified of the purpose and legal authority for the collection.

iii. **Accuracy of personal information**
    If a public body has personal information that it will use to make a decision directly affecting an individual, it must make reasonable efforts to ensure it is accurate and complete. There is a good business reason for doing this and it is required under FIPPA. Accordingly, public bodies need to have in place policies and procedures for ensuring that personal information they use to make decisions is not out of date, or otherwise inaccurate, or incomplete.

iv. **Access to and correction of personal information**
   Employers should understand that individuals have a right to request access to, and correction of, their own personal information. Employers can help citizens and employees exercise this right by knowing what processes to follow. The best approach is to have policy direction about how access will be provided, and how correction requests should be handled (typically, these may be sent to the Privacy Officer). This promotes consistency, quality and timeliness in decision-making.

v. **Retention and disposal of personal information**
   Under FIPPA, a public body must retain personal information for at least one year after it is used to make any decision that directly affects the individual the information is about. There is no retention limit specified in FIPPA, but in order to minimize

---

10 Employee policy guidance is also necessary in light of FIPPA’s requirement that a public body, with some exceptions, notify individuals of the purposes for collection of their personal information and provide certain other information. See s. 27 of FIPPA.

11 FIPPA requires that collection be directly from the individual the information is about, unless indirect collection is authorized by s. 27.

12 FIPPA, s. 28.

13 FIPPA, s. 31.
unauthorized collection, use and disclosure of personal information, a public body should not retain personal information that is no longer required for operational, legal or archival reasons. Policy guidance for employees is an important part of ensuring that retention schedules are adhered to.

Ministries have to ensure that their policy and practices also comply with applicable government information and records management policies and legislation (such as the Document Disposal Act). There may also be applicable records management rules or policies for Crown corporations or other public bodies. Further, legal requirements—including those imposed by insurers—may affect the retention period for personal information in many cases.

Policies should specify the appropriate method of disposal of personal information, both in hardcopy and electronic form. For example, special procedures need to be followed to remove information from electronic devices before disposal; simply deleting the data on these devices will not necessarily prevent its recovery.

vi. Responsible use of information and information technology

Under FIPPA, a public body must protect the personal information it holds by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. What is reasonable depends on the sensitivity of the information and a variety of other factors. The risk assessment and compliance considerations involved are outside the scope of this document. However, a public body must have in place policies and procedures for protecting personal information. An important function of such policies is to inform employees of what is required of them in order to protect personal information.

Public bodies must implement role-based access as a security control to limit who has access to what information. This entails, in accordance with the need-to-know and least privilege principles, ensuring that wherever practicable, employees have access only to the minimum amount of personal information they require to perform their employment duties. Access permissions should be documented, remain up-to-date and be assigned on a consistent basis, preferably by a central authority within the public body.

Due to technical limitations, it is not always possible to create an access control model that limits access on a strict need-to-know basis. In such cases, users should sign confidentiality agreements under which they agree only to access information that is necessary to fulfill their duties. System logs, if available, should be audited periodically to ensure that users are accessing information appropriately.

Information technology controls are particularly important in the context of common or integrated programs or data-linking initiatives involving public bodies. As these activities increase in scale, it will become increasingly more important for public bodies to use technology to protect personal information.

---

14 The nature and scope of any other records management and retention requirements is also beyond the scope of this document, and expert advice should be sought in order to ensure all requirements are met.
15 FIPPA, s. 30.
16 FIPPA, s. 33.1(e) and s. 33.2(e).
vii. **A process for handling privacy-related complaints**

Individuals have the right to challenge a public body’s compliance with applicable privacy legislation. Public bodies therefore should have processes in place for staff to follow in the event that individuals wish to complain about the public body’s personal information handling practices.

**c) Risk assessment tools**

Privacy risks evolve over time. Conducting regular risk assessments is an important part of any privacy management program. As noted earlier, services change, programs come and go, administrative structures evolve, and so on. These can all drive changes in personal information practices and risks. Proper use of risk assessment tools such as privacy impact assessments (PIAs) and security threat and risk assessments (STRAs) can help identify and repair associated problems, or prevent them from arising in the first place – fixing a privacy problem after the fact can be costly, especially where there has been a breach.

A PIA should be done for all new projects involving personal information and for any new collection, use, or disclosure of personal information. Further, FIPPA requires that all public bodies conduct a PIA for common or integrated programs or activities and data-linking initiatives. It defines a PIA as “an assessment that is conducted by a public body to determine if a current or proposed enactment, system, project, program or activity meets or will meet the requirements of Part 3” of FIPPA.¹⁷ FIPPA also authorizes the minister responsible for FIPPA to create specific PIA-related requirements.¹⁸ A sound privacy management program should, as with all other legislative and policy requirements, be reviewed regularly to ensure that it continues to meet the PIA requirements under FIPPA.

PIAs should also be conducted for significant modifications of existing systems, programs or activities. For example, the following modifications should trigger a new PIA:

- new types of personal information will be collected
- significant changes will be made in the way personal information is used or disclosed
- personal information will be linked with information from third parties
- system access is being changed so that new categories or groups of individuals will have access to personal information
- management or security of the personal information will be outsourced to a service provider
- the retention period for personal information will be changed

To ensure that the PIAs are conducted, public bodies should develop procedures for completing PIAs, which should involve the Privacy Officer from the outset. These procedures also should involve all affected operational areas, including IT managers and staff where electronic information systems are involved.

The same considerations apply to STRAs, tools that should be used to assist a public body to comply with security requirements under s. 30 of the FIPPA. STRAs should either form a part of a PIA or be performed separately but alongside a PIA where appropriate.

¹⁷ FIPPA, s. 69.
¹⁸ None were issued at the time of this guidance but public bodies should keep abreast of applicable requirements at all times.
d) Training

Training is very important. There are many examples of situations where a lack of awareness meant privacy issues were not identified, resulting in privacy breaches such as misdirected faxes, email or insecure records disposal.

Training and awareness are necessary because, in order for a privacy management program to be effective, employees must be actively engaged in privacy protection. Employees will be able to better protect privacy when they are able to recognize privacy issues as they arise.

A public body may have sound privacy controls in place, but if employees are not aware of them, the controls are of no real use. An effective privacy management program will enable all employees and officials to be aware of, and be ready to act upon, the public body's privacy obligations. If an urgent need arises, prompt communication of essential information must be disseminated to relevant employees as soon as is practical, without waiting for the next organized training session.

Privacy training should be mandatory for all employees, and should be tailored to their specific duties. Training should be ongoing, regular and sufficiently detailed and informative as to equip employees with the knowledge (and awareness) necessary to meet the public body's privacy obligations. The content of the training program should be periodically revisited and updated to reflect changes within the public body, to FIPPA and to industry best practices.

There are many ways in which a public body can deliver training. Examples include mandatory training modules on a public body intranet, small-group sessions, one-on-one training, monthly newsletters and privacy modules contained in public body policy training.

A public body should document its training processes. It should also measure participation and success of employees receiving the training, using objective and consistent measurements.

e) Breach and incident management response protocols

There have been numerous high-profile, large-scale, privacy breaches in BC in recent years. These have often involved the sensitive personal information of many individuals. When a breach occurs, it is important that it be contained and mitigated with urgency.

This can only be done effectively if the privacy management program includes procedures for managing breaches. The program should clearly assign responsibilities for containing, mitigating and reporting a breach. In a larger public body, this may require collaboration on the part of employees from different parts of the public body. Another key part of a privacy breach response protocol is assignment of responsibility for investigating the causes of the breach and ensuring the lessons learned are then incorporated into procedures, practices and employee training.

The OIPC expects that, as part of their FIPPA duty to protect personal information against, among other risks, unauthorized disclosure or use, public bodies will promptly report privacy breaches to the OIPC where appropriate.

For more guidance on privacy breach management, refer to the OIPC's Privacy Breach Checklist, Breach Notification Assessment Tool, and Key Steps in Responding to Privacy Breaches. Other similar resources are available on other Canadian information and privacy commissioner websites identified in Appendix A.
f) Service provider management

Throughout the BC public sector there are many kinds of service provider relationships that involve personal information. They range from wholesale outsourcing of government programs, such as health insurance or payroll processing, to workplace harassment investigations by human resource consultants. Any time personal information is disclosed to or used by a service provider under such an arrangement, the public body remains responsible for privacy compliance. The service provider may well have obligations under the Personal Information Protection Act, but this does not, in the OIPC’s view, affect the public body’s responsibilities under FIPPA.19

A privacy management program should, therefore, include procedures for ensuring compliance by contractors with relevant FIPPA obligations and with their contractual obligations to the public body. In larger public bodies, especially, program procedures should ensure collaboration between the Privacy Officer and the public body’s procurement and contracting staff during all relevant phases.

An important consideration for this aspect of the program should be FIPPA’s requirements for public bodies that, with some exceptions, prohibit disclosure of personal information outside Canada or access to it from outside Canada. A public body that wishes to contract with a service provider must ensure that it meets these requirements. This may be particularly relevant where a public body is considering contracting with a cloud services provider, including the provision of email, office applications, and software services. Cloud services very often involve the storage of personal information outside Canada or access to it from outside Canada. Careful inquiries must therefore be made before entering into cloud services arrangements involving personal information.20

Please note that FIPPA contains some exceptions to the restrictions on storage or access to personal information outside Canada. For example:

- public bodies may disclose personal information outside Canada for the purpose of authorizing, administering, processing, verifying or canceling a payment to be made to or by a public body (this allows public bodies to accept credit card payments);21 and
- public bodies may temporarily disclose personal information to service providers outside Canada for the purposes of installing, implementing, maintaining, repairing, trouble-shooting or upgrading their systems (this allows foreign service providers to get temporary access to systems under the listed circumstances).22

Privacy requirements for service provider relationships should include the following:

- clear contractual requirements, including: limiting use and disclosure of personal information by the service provider to specified contractual purposes; taking reasonable security measures to protect personal information; requiring compliance

---

19 FIPPA defines ‘employee’ to include, in relation to a public body, “a service provider”, which is defined as “a person retained under a contract to perform services for a public body”. In turn, “person” includes corporations, individuals and partnerships. Accordingly, a ‘service provider’, since it is treated as an ‘employee’ of the public body to which it is providing services, will have direct privacy obligations under FIPPA. This does not mean, however, that the public body is absolved of responsibility.

20 For more on guidance about using cloud services please consult: http://www.oipc.bc.ca/guidance-documents/142?.

21 FIPPA, s. 33.1(1)(i.1).

22 FIPPA, s. 33.1(1)(p).
with privacy policies and controls of the public body, including with respect to storage, retention and secure disposal; and requiring notice to the public body in the event of a privacy-related contract breach;

- controls on sub-contracting by the service provider;
- training and education for all service provider employees with access to sensitive personal information;
- requirement for the service provider to require its employees to agree that they will comply with privacy obligations; provisions addressing the sale of, or change of control in, the business, including through insolvency or bankruptcy;
- provisions enabling the public body to review or audit the service provider’s compliance at any time;
- indemnification of the public body from any liability that might be asserted where the service provider is at fault; and
- sanctions for contract breach (including contract termination, and return or destruction of personal information, where there is a material breach).

The Provincial Government publishes a useful Privacy Protection Schedule for contracts, which covers most of the above requirements.23

g) Communicating with individuals and demonstrating accountability

A number of FIPPA’s requirements involve communication between public bodies and the individuals whose personal information they collect, use or disclose, including the public body’s own employees. These include giving notice of collection, responding to requests by individuals for access to their own personal information, requests for access to records where someone else’s personal information is involved and requests for correction of personal information.24 As another example, the program should address giving notice to an individual after his or her personal information is disclosed without consent for compelling health or safety reasons.25 A final example is FIPPA’s requirement that a public body notify an individual where the public body intends to give access to her or his personal information in response to a freedom of information request.26

A privacy management program should, therefore, include requirements related to these FIPPA rules. It should also include a procedure for informing individuals of their privacy rights and of the public body’s program controls. All external communications should be expressed in clear, understandable language.

These are key considerations given FIPPA’s explicit goal of promoting the openness and accountability of public bodies. Openness about a public body’s privacy policies, practices and compliance measures is part of its accountability as a public sector organization and its accountability under FIPPA.

24 Obligations under FIPPA to maintain personal information banks or make other privacy-related information available should also be addressed for the privacy management program to be comprehensive.
25 See s. 33.1(1)(m). Also note that public interest disclosures of personal information under s. 25 require advance notice to affected individuals, “if practicable” (notice must be given afterward if advance notice is not practicable).
26 See s. 23(1).
At a minimum, the Privacy Officer should conduct periodic assessments to ensure key processes are being respected. A privacy management program should include compliance checklists, which themselves need to be reviewed regularly as part of ongoing program review.

To meet its FIPPA obligations and be accountable for its privacy practices, a public body should monitor, assess and revise its privacy management program regularly and consistently. This is the only way the program can remain relevant and effective. This part outlines the ways in which a privacy management program may be maintained in order to ensure its currency and effectiveness.

1 Develop an Oversight and Review Plan

The Privacy Officer should develop a plan to review the program periodically. The plan should set out how and when the Privacy Officer will monitor and assess the program’s effectiveness against FIPPA and the public body’s policies. To do this properly, a plan should set out performance measures and scoring criteria.

Assessment of a privacy management program also requires a documented assessment of any changes in the public body’s operating environment. This will include review of any relevant changes in the public body’s powers, duties or functions; statutory or policy framework; organizational or management structures; budget resources; or operating programs or activities.

2 Assess and Revise Program Controls

The effectiveness of program controls should be monitored, periodically audited and, where necessary, revised. Monitoring is an ongoing process and should address at a minimum the following questions:

- what are the latest privacy or security threats and risks?
- are the program controls addressing new threats and reflecting the latest complaint or audit findings, or guidance, of the OIPC?
- are new services being offered that involve increased collection, use or disclosure of personal information?
- is training occurring, is it effective, are policies and procedures being followed?

If problems are found, they should be documented and addressed by the appropriate officials, in collaboration with the Privacy Officer.

For critical or high-risk processes, periodic internal or external audits can be useful in assessing the effectiveness of a privacy program. At a minimum, the Privacy Officer should conduct periodic assessments to ensure key processes are being respected. A privacy management program should include compliance checklists, which themselves need to be reviewed regularly as part of ongoing program review.
Even a public body that has a fairly mature privacy management program needs to ensure it is taking reasonable steps to comply with FIPPA. A public body should regularly assess its program controls, discussed in Part A, in a systematic and thorough way. The Privacy Officer should consider whether assessment results require changes to the public body's program controls. This is a critical responsibility. Any necessary changes should be made promptly and, where critical, must be communicated to employees promptly, or otherwise through the ongoing training discussed above.

The Privacy Officer should review the program controls regularly and at the very least:

- ensure the public body's personal information inventory is updated, and that new collections, uses and disclosures of personal information are identified and evaluated;
- revise policies 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;
- treat privacy impact assessments and security threat and risk assessments as evergreen documents, so that changes in privacy and security risks are always identified and addressed;
- review and modify training on a periodic basis as a result of ongoing assessments and communicate changes made to program controls;
- review and adapt breach and incident management response protocols to implement best practices or recommendations and lessons learned from post-incident reviews;
- review and, where necessary, fine-tune requirements in contracts with service providers; and
- update and clarify external communications.

**Conclusion**

Public bodies need to be vigilant in the area of privacy because public trust and confidence are at stake. Privacy management programs must be documented and transparent. In the event of a privacy or security breach, public bodies will want to be able to point to the safeguards they have in place to try to prevent such breaches and how they will be assessed and revised once a breach has occurred. This will help to allay not only the public’s concerns but will also answer questions the OIPC will ask should it decide that an audit or investigation is warranted.

There is not a one-size-fits all privacy management program. The building blocks are scalable and should be tailored to the size and mandate of the public body and the amount and nature of the personal information it has in its custody and control.

It is hoped that the guidance in this document will assist public bodies in BC to ensure legal compliance, to meet privacy and security best practices and demonstrate accountability to citizens. The Office of the Information and Privacy Commissioner for BC will be assessing the privacy management programs of public bodies in future investigations and audits.
# Privacy Management Program – At A Glance

## A. Building Blocks

<table>
<thead>
<tr>
<th>PUBLIC BODY COMMITMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive-level support</td>
</tr>
</tbody>
</table>
| Privacy Officer (Head)  | • Role is defined and is fundamental to business decision-making process.  
                          | • Role and responsibilities for monitoring compliance are clearly identified and communicated throughout the public body.  
                          | • Responsible for the development and implementation of the program controls and their ongoing assessment and revision.  
                          | • Adequate resources are identified.  
                          | • Public body structure supports the ability of staff to monitor compliance and foster a culture of privacy within the public body.  
                          | • Ensures privacy protection is built into every major function involving the use of personal information. |
| Reporting               | Reporting mechanisms should be established, and they need to be reflected in the public body’s program controls. |

<table>
<thead>
<tr>
<th>PROGRAM CONTROLS</th>
</tr>
</thead>
</table>
| Personal Information Inventory | The public body is able to identify:  
                                   | • the personal information in its custody or control,  
                                   | • its authority for the collection, use and disclosure of the personal information, and  
                                   | • the sensitivity of the personal information. |
| Policies          | i. Collection, use and disclosure of personal information, including requirements for consent and notification  
                          | ii. Indirect collection of personal information  
                          | iii. Accuracy of personal information  
                          | iv. Individual access to and correction of personal information  
                          | v. Retention and disposal of personal information  
                          | vi. Responsible use of information and information technology, including administrative, physical and technological security controls and appropriate access controls  
                          | vii. A process for responding to privacy-related complaints |
| Risk Assessment Tools Training Breach and incident management response protocols Service Provider management External communication |
### B. Ongoing Assessment and Revision

**OVERSIGHT AND REVIEW PLAN**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop an oversight and review plan</td>
<td>Privacy Officer should develop an oversight and review plan on an annual basis that sets out how s/he will monitor and assess the effectiveness of the public body's program controls.</td>
</tr>
</tbody>
</table>

**ASSESS AND REVISE PROGRAM CONTROLS AS NECESSARY**

- Update personal information inventory
- Revise policies
- Treat risk assessment tools as evergreen
- Modify training and education
- Adapt breach and incident response protocols
- Fine-tune service provider management
- Improve external communication
This appendix identifies resources that may assist public bodies in designing, implementing and maintaining their public body privacy management program.

**Privacy Breaches: Tools and Resources** (includes: *Key Steps in Responding to Privacy Breaches; Privacy Breach Checklist; Privacy Breach Management Policy Template; Breach Notification Assessment Tool*):

http://www.oipc.bc.ca/guidance-documents/1428

**Privacy Emergency Kit**: provides guidance for sharing personal information in an emergency, prepared by the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner for BC

http://www.oipc.bc.ca/guidance-documents/1538

**Security Self-Assessment Tool**: This document will help you assess your organization’s security measures and offers guidance on minimum security requirements in 17 different categories. Produced jointly by the Office of the Privacy Commissioner of Canada, the Office of the Information and Privacy Commissioner of Alberta and the Office of the Information and Privacy Commissioner for B.C.

http://www.oipc.bc.ca/guidance-documents/1439

**Cloud computing for public bodies**: This document outlines how FIPPA applies to cloud computing, including the requirement that data only be stored and accessed in Canada.

http://www.oipc.bc.ca/guidance-documents/1427

**Protecting personal information outside the office**: Personal information can more easily be lost or compromised when it’s outside your office. Common sense measures can and should be taken to reduce risks to personal information in such situations.

http://www.oipc.bc.ca/guidance-documents/1447