SECURITY

Updated February 2023

Accountable Privacy Management in BC's Public Sector

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Contents

This document provides step-by-step guidance for British Columbia public bodies on how to implement effective Privacy Management Programs (PMP).

A PMP 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 effects of new and emerging technologies on personal privacy, especially digital solutions for managing personal information. An investment in privacy protection today can help prevent a costly data breach tomorrow.

As of February 1, 2023, BC's *Freedom of Information and Protection of Privacy Act* (FIPPA) requires all public bodies to develop a PMP in accordance with mandatory PMP directions issued by the Minister of Citizens' Services. The mandatory PMP directions tell public bodies what they must do, at a minimum, to create and maintain a PMP that complies with FIPPA.

To help public bodies comply with the mandatory PMP directions, the Ministry of Citizens' Services has published guidelines applicable to non-ministry public bodies, as well as a Privacy Management and Accountability Policy that is applicable to ministries.

This guidance document, which provides information on the OIPC's expectations of public bodies in fulfilling the PMP requirement, is meant to complement the mandatory PMP directions and to make suggestions on how to comply with them.

Purpose of this guidance document

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.

The first part of this document outlines the fundamentals of a PMP, including an organizational commitment to privacy compliance, program controls, risk assessment and training. The second part of the document provides suggestions for how public bodies can review, revise and maintain their PMPs on an ongoing basis.

What is accountability?

Accountability in relation to privacy means accepting responsibility for protecting personal information. To demonstrate accountability for privacy and personal information, a public body should have demonstrable and comprehensive policies, procedures and practices in place that comply with FIPPA. These practices, taken as a whole, constitute a PMP.

While the concept of accountability may appear to be straightforward, constructing a PMP requires thoughtful planning. Employees should be aware of and understand how the PMP

applies to them. The public should have access to meaningful information about the public body's PMP.

Steps to setting up the program

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

- 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);
- ensure oversight by executive management through a project lead;
- to the extent necessary, involve human resources, risk management, internal audit and IT personnel;
- if necessary, obtain outside privacy expertise;
- obtain and document information to assess compliance, including through staff interviews, file reviews and IT system reviews;
- regularly report to executive on progress and implement any resulting direction from executive as appropriate in accordance with FIPPA;
- report to executive on any identifiable risk and compliance issues;
- provide a final report of all findings to executive with a full mapping of findings against FIPPA's requirements; and
- any other steps that might, in light of the public body's own situation, be desirable to document its current state of compliance and future activities.

PMP essentials

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 purpose of this guidance document is for the OIPC to provide scalable solutions for public bodies large and small to help them to fulfill their significant and legally-binding FIPPA obligations with respect to PMPs.

Accountability has several important elements. FIPPA requires that each public body have a 'head' (as defined in Schedule 1 of FIPPA) who is accountable for the privacy requirements in 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. The head should ensure that there is someone responsible for FIPPA compliance and awareness within the public body on a day-to-day basis.

Demonstrating commitment to privacy compliance

The foundation of a PMP is for public bodies to develop a comprehensive internal governance structure that prioritizes privacy compliance and fosters a privacy-respectful culture. Structures and processes are key components of a PMP, but public bodies should create and maintain a culture of privacy awareness. This is of fundamental importance to their ability to meet privacy challenges as they arise.

Demonstrating senior management commitment and support

Executive-level support is at the heart of a privacy-respectful workplace culture and of any successful PMP. Executive commitment to FIPPA compliance and to good practices increases the likelihood that the public body's PMP will be effective.

To actively champion a PMP, executives at the public body should ensure that all resources necessary to develop, implement, monitor and adapt the PMP are available to the designated head of the public body under FIPPA. Public bodies face competing demands for public resources. However, compliance with FIPPA is mandatory.

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 a public body's privacy practices are important; the legislative power of being able to compel citizens to surrender their personal information depends on that trust and confidence.

Designate and empower a Privacy Officer

The Ministry mandatory PMP directions require that the head of a public body designates an individual(s) to be responsible for the following:

a. being a point of contact for privacy-related matters such as privacy questions or concerns;
b. supporting the development, implementation, and maintenance of privacy policies and/ or procedures; and
c. supporting the public body's compliance with FIPPA.

In other words, the head or their delegate should ensure the public body's compliance with FIPPA generally, and is responsible for management and direction of the PMP.[1] It does not matter whether the Privacy Officer is an executive level manager of a provincial government

[1] Further, when a public body designates someone as its Privacy Officer, it must ensure that delegations of the duties and functions of the head under FIPPA are valid.

ministry or the administrator of a small local government—someone must be responsible for the public body's privacy compliance and practices.[2]

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 PMP;
- 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 assume other duties without affecting their ability to discharge their 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. Public bodies can achieve this objective as part of the initial assessment and design of the PMP, with appropriate resources, including staff who can dedicate the time it will take to properly implement the PMP. Funding the PMP should become a non-discretionary component of the public body's annual budget cycle.

Compliance reporting

A PMP's controls need to include several types of reporting mechanisms. The goal should be to ensure that the Privacy Officer and executive management know whether the program is

[2] Public bodies should keep in mind that designation of a Privacy Officer does not diminish their ultimate accountability for compliance with FIPPA.

functioning as expected, how and why it is not, and what the proposed solutions for improvement are.

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. A public body may decide to hire a third party to perform an audit when, for example, 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.

Another key kind of reporting relates to security breaches or citizen privacy complaints. These require escalation 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 may include information technology professionals, security experts, information managers, legal advisers and communication advisers.

A PMP should clearly define when and how a public body should escalate their response to a privacy incident, and to whom. FIPPA requires that staff inform the head of the public body of any unauthorized disclosure of personal information.[3] In instances of other privacy complaints, staff at public bodies should generate progress reports about the handling of a matter to the Privacy Officer or their delegate. This is necessary to ensure that a public body is following its documented process. It is useful to evaluate the robustness of the escalation and reporting process by conducting a test run of privacy breach identification, escalation, and containment protocols.

Program Controls

Program controls help ensure that public bodies implement internal governance mechanisms that help them meet their obligations to protect personal information.

Personal information inventory

A thorough personal information inventory is a fundamental and 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 will be extremely difficult to comply with FIPPA.

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.

[3] See s. 30.5 of FIPPA.

Public bodies will need to ensure that their inventory covers only personal information as Schedule 1 of FIPPA defines it: "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.[4] Generally speaking, if information either identifies an individual (including through a unique identifier, biometric, or metadata) 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 should provide, on a ministry-by-ministry basis, information about records of personal information in the custody or control of each ministry. The directory should also include information about the use of those records by each ministry. Further requirements exist, including providing details about the information-sharing agreements of each ministry and about which PIAs each ministry has completed.[5]

Further, public bodies other than ministries also have obligations to publish information about their personal information holdings and uses. Their directories should describe the kind of personal information they hold, the categories of individuals whose information they hold, the authority and purposes for collection, and who the public body discloses personal information to, including contractors working on behalf of the public body.[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, who the public body discloses it to, 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 to assess existing compliance with FIPPA's rules overall. It is also necessary to design and implement an effective PMP. In other words, every aspect of a sound and effective PMP begins with this inventory.

[4] Section 8 of BC's *Interpretation Act* mandates a "fair…large and liberal" interpretation of statutes.

[5] FIPPA, s. 69 https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00_multi#section69.

[6] FIPPA, s. 69(6).

Each public body should 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 the public body stores personal information (including service providers);
- purposes for which the public body collects, uses, and discloses personal information; and
- the sensitivity of the personal information the public body holds.

Compliance policies

The Ministry directions require that public bodies make available to employees, and where practical, to the public, privacy policies and any documented privacy processes.

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

- purposes for which the public body collects, uses and discloses personal information;
- authority for the collection, use and disclosure of personal information;
- requirements for consent and notification;
- accuracy of personal information;
- individual access to and correction of personal information;
- retention and disposal of personal information;
- responsible use of information and information technology, including administrative, physical and technological security controls, and appropriate access controls; and
- a documented process for handling privacy-related complaints and privacy breaches (this is mandatory under the Ministry directions).

Risk assessment tools

Privacy risks evolve over time. Conducting regular risk assessments is an important part of any PMP. 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 PIAs and security threat and risk assessments (STRAs) can help public bodies to identify and remediate risks, or to prevent them from arising in the first place.

Privacy Impact Assessments (PIAs)
FIPPA authorizes the minister responsible for FIPPA to create specific PIA-related directions for ministries (read the PIA directions for ministries) and non-ministry public bodies (read the PIA directions for non-ministry public bodies). To assist public bodies in fulfilling their obligations to complete PIAs under the directions, the Ministry of Citizens' Services has published detailed PIA guidance on its website. Public bodies should ensure employees responsible for privacy at the public body are familiar with this information and take steps to comply with the PIA directions.

Security Threat and Risk Assessments (STRAs)
A STRA is a tool that public bodies should use to evaluate their compliance with the requirement in s. 30 of FIPPA, which states:

> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal.

OIPC orders have established the meaning of "reasonable security arrangements." In short, for public bodies to meet their legislative obligations, they must take measures that are "objectively diligent and prudent in all of the circumstances."[7] Further, "the nature of the personal information involved and the seriousness of the consequences of its unauthorized disclosure are factors to be taken into account in assessing the reasonableness of security arrangements."[8]

To help fulfill the obligations that FIPPA imposes on public bodies to protect personal information, the Ministry of Citizens' Services has published detailed information about STRAs, including a STRA workbook template.

Privacy training
The Ministry's PMP directions require that public bodies establish privacy awareness and education activities to ensure employees are aware of their privacy obligations.

Privacy training should be *mandatory* for all employees, and should be scaled to meet the volume and sensitivity of personal information in the custody or under the control of the of the public body, and should be undertaken at timely and reasonable interval. 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.

[7] See "Sale of Provincial Government Computer Tapes Containing Personal Information, Re, 2006 CanLII 13536 (BC IPC)," https://canlii.ca/t/1n468, at paragraph 49.
[8] See https://www.oipc.bc.ca/special-reports/1271 at page 110.

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.

For more information, see the Ministry's Privacy and Information Management Training website. That website includes access to a free online training course to help public body employees to meet their FIPPA obligations.

Breach and incident management response protocols

When a privacy breach occurs, it is important that it be contained and mitigated with urgency. This can only be done effectively if the PMP includes procedures for managing breaches, knowing that the Ministry's PMP directions require that public bodies have a documented process for responding to privacy complaints and privacy breaches.

A public body's breach management process should assign responsibilities to specific individuals within the public body who are responsible 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 management process is making sure that someone at the public body is responsible for investigating the causes of the breach and ensuring the lessons learned are then incorporated into procedures, practices, and employee training.

For more guidance on privacy breach management, refer to the OIPC's *Privacy Breaches: tools and resources for public bodies*.

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 affect the service provider's responsibilities under FIPPA when it is providing services to a public body.[9]

[9] 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,

A PMP should, therefore, include procedures for ensuring compliance by contractors for their FIPPA obligations. 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.

A public body that wishes to contract with a service provider should ensure that it meets FIPPA 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. Careful inquiries should therefore be made before entering into cloud services arrangements involving personal information.

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 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;
- methods to ensure that service providers are informed of their privacy obligations (e.g., awareness activities, contractual terms that address privacy obligations), per the Ministry directions;
- 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 Ministry publishes a useful Privacy Protection Schedule for contracts, which covers most of the above requirements.

individuals, and partnerships. Accordingly, a 'service provider', because it is an 'employee' of the public body to which it is providing services, will have direct privacy obligations under FIPPA.

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. As another example, the program should address giving notice to an individual after their personal information is disclosed without consent for compelling health or safety reasons under Part 3 of FIPPA. A final example is FIPPA's requirement that a public body notify an individual where the public body intends to give access to their personal information in response to a freedom of information request under Part 2 of FIPPA. A PMP should also include a procedure for informing individuals of their privacy rights and of the public body's program controls.

These are key considerations given FIPPA's explicit goal of promoting the openness and accountability of public bodies. Transparency about a public body's privacy policies, practices and compliance measures is an important part of its accountability under FIPPA.

Ongoing Assessment and Revision

To meet its FIPPA obligations and be accountable for its privacy practices, a public body should monitor, assess, and revise its PMP regularly and consistently. The Ministry directions require that public bodies put in place a process for regularly monitoring the PMP and updating as required, to ensure it remains appropriate to the public body's activities and is compliant with FIPPA. This is the only way the program can remain relevant and effective. This part outlines the ways in which a PMP may be maintained in order to ensure its currency and effectiveness.

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 PMP 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.

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 PMP 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 PMP needs to ensure it is taking reasonable steps to comply with FIPPA. A public body should regularly assess its program controls, discussed 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, should be communicated to employees promptly, or otherwise through the ongoing training discussed above.

The Privacy Officer should review the program controls regularly and:

- 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, or as a result of environmental scans;
- treat PIAs and STRAs 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 around privacy because public trust and confidence are at stake. Public bodies should document their PMPs to demonstrate their compliance with FIPPA. 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 they should update their PMPs after a breach has occurred with any new measures that might help to prevent a similar breach from taking place in the future.

There is not a one-size-fits-all PMP. 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.

The purpose of this document is to 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 PMPs of public bodies in future investigations and audits.

PO Box 9038 Stn. Prov. Govt. Victoria BC V8W 9A4 | 250-387-5629 |

Toll free in BC: 1-800-663-7867 info@oipc.bc.ca | oipc.bc.ca | @BCInfoPrivacy