Privacy Management and Accountability Policy

Corporate Information and Records Management Office

Privacy, Compliance and Training Branch

Ministry of Citizens' Services

Version 4.0

BRITISH COLUMBIA

Revision History

V.1: May 2016
V.2: January 2019
V.3: November 2019
V.4: September 2022

Table of Contents

1.0 Introduction

Good privacy practices enable public bodies to demonstrate accountability and enhance services to citizens. The Privacy Management and Accountability Policy (PMAP) is the framework for the Province of British Columbia's privacy management program. It describes privacy management accountabilities, strengthens government's ability to protect the privacy of individuals' Personal Information and helps ensure that ministries are compliant with the privacy requirements of the Freedom of Information and Protection of Privacy Act (FOIPPA). PMAP identifies the mandatory assessment tools and agreements, reporting and audit requirements, and the policies and procedures that ministries must follow. All these measures work together to support compliance with FOIPPA.[1]

PMAP outlines the privacy-related requirements of all Employees working for ministries within the Province of British Columbia. As defined in FOIPPA, a public body's "Employee" includes both volunteers and Service Providers. PMAP outlines specific accountabilities of Deputy Ministers, Ministry Privacy Officers (MPOs), and the Corporate Information and Records Management Office (CIRMO). Deputy Ministers are responsible for supporting the continuous improvement of privacy practices and the responsible collection, use, disclosure, storage, access, retention and disposal of Personal Information in their ministry. Deputy Ministers are also responsible for ensuring that PMAP is communicated to all Employees in their ministry.

The Privacy, Compliance and Training Branch (PCT) in CIRMO, within the Office of the Chief Information Officer (OCIO), is B.C. government's corporate privacy office. PCT encourages positive privacy practices through reviews, training, policy development and expert advice; supports responsible information management through the resolution of actual and suspected information incidents; and promotes continuous improvement through the assessment of the maturity of ministry information management practices. MPOs are the point of contact for privacy management practices, processes and expertise in their ministries and are a rich resource for Employees seeking to incorporate privacy principles and obligations into their work. It is the responsibility of all Employees to be stewards of Personal Information, and PMAP helps to support the expansion of positive privacy practices within each ministry.

[1] Note that, in some cases, legislation other than FOIPPA may also govern the collection, use, disclosure, storage, access, retention and disposal of Personal Information.

1.1 Scope

PMAP applies to all ministries in the Province of British Columbia, including Ministry Deputy Ministers, Ministry Privacy Officers, Employees, and the Corporate Information and Records Management Office.

1.2 Effect

The requirements and accountabilities of this policy take effect immediately upon publication of the policy, except for requirements related to relevant policies not yet in place. When published, the related policies will set out relevant effective dates.

1.3 Authority

FOIPPA mandates how Personal Information may be collected, used and disclosed by public bodies in British Columbia. The authority for PMAP stems from Chapter 12 of the Core Policy and Procedures Manual (Core Policy). Core Policy requires ministry compliance with government's privacy management program outlined in PMAP.

1.4 Legal Considerations

FOIPPA protects personal privacy by prohibiting the unauthorized collection, use, disclosure, storage and disposal of Personal Information by government ministries and other public bodies. PMAP does not replace or limit a ministry's obligations under FOIPPA, including any regulation made under it; rather, PMAP supports compliance with the privacy requirements of FOIPPA. Ministries must ensure they meet all their obligations under FOIPPA.

1.5 Advice on this Policy

PCT within CIRMO is the Province of British Columbia's central privacy office. For advice on PMAP, call or email PCT at 250-356-1851 or privacy.helpline@gov.bc.ca.

2.0 Policy Requirements

2.1 Accountability for Privacy Management

Deputy Ministers

2.1.1 Deputy Ministers must designate an individual responsible for privacy within their respective ministry and provide the Contact Information of this individual to CIRMO within the OCIO. This individual will be designated the MPO. Deputy Ministers may, at their discretion, designate an additional MPO for a specific area within their ministry that provides corporate services for the Province of British Columbia (e.g., Public Service Agency, Government Communications and Public Engagement) or when appropriate given the volume and sensitivity of Personal Information held by their ministry.

Employees

2.1.2 Employees may develop ministry-specific policies and procedures to support this policy or compliance with FOIPPA in collaboration with MPOs and in keeping with ministry processes. Any such ministry-specific policies and procedures must be submitted to CIRMO for review during development of the policy.

Ministry Privacy Officers

2.1.3 MPOs are accountable to be the single point of contact for privacy in their ministry and remain accountable for any assigned roles and responsibilities that they delegate.

2.1.4 MPOs may develop ministry-specific policies and procedures to support this policy or compliance with FOIPPA. Any such ministry-specific policies must be submitted to CIRMO for review during development of the policies.

2.1.5 MPOs must communicate substantive changes to PMAP to relevant ministry Employees as determined by the MPO.

Corporate Information and Records Management Office

2.1.6 CIRMO must review PMAP annually and update as appropriate with input from MPOs and other stakeholders and inform MPOs of all significant changes.

2.1.7 CIRMO must establish and chair a Privacy Management Community of Practice to facilitate knowledge, experiences and best practices between privacy professionals across government.

2.1.8 CIRMO must convene a forum for MPOs to facilitate dialogue between the MPOs, CIRMO and other interested parties.

2.1.9 CIRMO must provide orientation for new MPOs regarding their role and responsibilities under PMAP.

2.1.10 CIRMO may develop privacy-related policies, guidance, guidelines and templates as necessary to support this policy or compliance with FOIPPA.

2.2 OIPC Engagement

Employees

2.2.1 Employees must engage with CIRMO before any engagement with the Office of the Information and Privacy Commissioner (OIPC) on matters relating to privacy and must include CIRMO in any engagement with the OIPC.

2.2.2 Employees must inform CIRMO and their MPO when their ministry has been contacted by the OIPC on matters relating to privacy.

Ministry Privacy Officers

2.2.3 MPOs must inform CIRMO when their ministry has been contacted by the OIPC on matters relating to privacy.

2.2.4 MPOs must engage CIRMO prior to any engagement with the OIPC on matters relating to privacy and must include CIRMO in any engagement with the OIPC.

Corporate Information and Records Management Office

2.2.5 CIRMO is responsible for managing the relationship of government ministries with the OIPC on matters related to privacy.

2.2.6 CIRMO must support MPOs and Employees to determine if engagement with the OIPC on matters related to privacy is appropriate, and if so, CIRMO must support ministries in their engagement with the OIPC.

2.3 FOIPPA Delegation

Deputy Ministers

2.3.1 The head of a public body may use a FOIPPA Delegation Instrument if they wish to delegate any duties, powers or functions of the head under FOIPPA to the MPO or any other person.

Ministry Privacy Officers

2.3.2 MPOs must maintain any current FOIPPA Delegation Instruments for their ministry and provide new and updated copies to CIRMO.

Corporate Information and Records Management Office

2.3.3 CIRMO must inform MPOs if CIRMO receives a new or updated FOIPPA Delegation Instrument pertaining to Part 3 of FOIPPA.

2.4 Education and Awareness

Employees

2.4.1 Employees must complete training on the appropriate collection, use, disclosure, storage and disposal of Personal Information as prescribed by CIRMO, i.e., the IM117 course offered through the Public Service Agency. An exemption may be granted by CIRMO for extenuating circumstances.

2.4.2 Employees must complete the ministry-specific training or awareness activities referenced in s.2.4.4, s.2.4.7 and s.2.4.8, when applicable.

2.4.3 Employees, including Service Providers and volunteers, who collect or create Personal Information must complete privacy training developed by CIRMO, unless granted an exemption by CIRMO. The training is on the appropriate collection, use, disclosure, storage, access, retention and disposal of Personal Information, i.e., the FOIPPA Foundations course. This training must be completed prior to providing any service that involves Personal Information. Training referred to in s.2.4.1 may be applied towards this requirement (where it has been documented).

2.4.4 Employees may develop ministry-specific training to support this policy or compliance with FOIPPA in collaboration with MPOs and in keeping with ministry processes. Any such ministry-specific training must be submitted to CIRMO for review during development of the training.

Ministry Privacy Officers

2.4.5 MPOs must develop, maintain and review internal processes to ensure all Employees take the mandatory training or complete the awareness activities referred to in s.2.4.1 and s.2.4.2, as applicable.

2.4.6 MPOs must develop, maintain and review internal processes to:

ii. Document Service Providers and volunteers who have access to Personal Information; and
ii. Ensure that the Service Provider and volunteer training requirements referred to in s.2.4.3 are properly applied.

2.4.7 MPOs may, in collaboration with CIRMO, develop ministry-specific privacy training to support PMAP and/or privacy-related matters.

2.4.8 MPOs must develop, maintain and review internal processes to ensure Employees who handle high risk or sensitive Personal Information within information systems or programs are aware of their privacy obligations. MPOs may use resources developed in collaboration with CIRMO or may use tools developed by CIRMO (once made available).

2.4.9 Once Ministry-specific training or awareness activities referred to in s.2.4.4, 2.4.7 and/or s.2.4.8 are developed, MPOs must ensure that the required activities are completed by all appropriate Employees within a timeline determined by the MPO.

Corporate Information and Records Management Office

2.4.10 CIRMO must develop training to support the appropriate collection, use, disclosure, storage and disposal of Personal Information (e.g., the privacy training referenced in s.2.4.1 and s.2.4.3).

2.5 Privacy Impact Assessments

Employees

2.5.1 Employees must conduct Privacy Impact Assessments (PIAs) in accordance with the PIA Directions as issued by the Minister responsible for FOIPPA, including any supplementary assessments, where necessary.

2.5.2 Employees must conduct PIAs during the development of any proposed enactment, system, project, program or activity of the ministry, or any proposed changes to an enactment, system, project, program or activity.

2.5.3 Employees must provide PIAs to their MPO. The Employee or the MPO must then submit the PIA to CIRMO. Employees responsible for preparing PIAs with respect to new or amended enactments may submit their PIAs directly to CIRMO. A PIA is not complete until it has been fully signed by all parties as required in the appropriate PIA Template as referenced in the PIA Directions.

2.5.4 Employees who are responsible for the activities outlined in the PIA must implement any mitigation or risk response strategies identified in the PIA with the support of their MPO (see s.2.5.8).

2.5.5 Employees may consult directly with CIRMO regarding PIAs in limited circumstances and in consultation with their MPO (see s.2.5.11).

Ministry Privacy Officers

2.5.6 MPOs must develop, maintain and review internal processes to support the completion of PIAs in their ministry. A PIA is not complete until it has been fully signed by all parties as required by the appropriate PIA Template as referenced in the PIA Directions.

2.5.7 MPOs must develop, maintain and review internal processes to ensure the reasonable completion of any mitigation or risk response strategies identified in PIAs within their ministry.

2.5.8 MPOs must support program areas, where necessary, in the reasonable implementation of any mitigation or risk response strategies identified in PIAs within their ministry.

2.5.9 MPOs must ensure that a copy of each completed and signed PIA is provided to CIRMO in the manner and form directed by CIRMO for retention and for entry into the Personal Information Directory (PID).

Corporate Information and Records Management Office

2.5.10 CIRMO must review and comment on all PIAs submitted by ministries. In certain circumstances, CIRMO may reassign their responsibilities relating to PIAs (e.g., for PIAs that do not involve personal information).

2.5.11 CIRMO may consult directly with Employees, in limited circumstances, and with the Employees and the MPO (see s.2.5.5). In such cases, there may be exceptions to the MPO accountabilities in s.2.5 when Employees consult directly with CIRMO.

2.6 Agreements

Employees

2.6.1 Employees must complete Information Sharing Agreements (ISAs) in accordance with the ISA Directions and with consideration to the ISA Guidance, unless granted an exemption by CIRMO. An ISA is not complete until it has been fully signed by all required parties as referenced in the ISA Directions.

2.6.2 Employees must complete Research Agreements (RAs) in accordance with section 33(3)(h) of FOIPPA.

2.6.3 Employees must complete Common or Integrated Program/Activity Agreements (CPAs and IPAs) and associated PIAs in accordance with section 69 of FOIPPA and section 12 of the FOIPP Regulation and where applicable.

2.6.4 Employees must consult their MPO (or other role identified in accordance with s.2.6.14) before entering into an ISA with a private sector organization (outside of a contractual relationship).

2.6.5 Employees must notify their MPO of all completed ISAs, CPAs and IPAs to allow the MPO to report them to CIRMO for entry into the PID.

2.6.6 Employees must notify their MPO of all completed Research Agreements (RAs).

2.6.7 Employees must notify their MPO when there are any substantive changes to an ISA, RA, CPA or IPA.

Ministry Privacy Officers

2.6.8 MPOs must develop, maintain and review internal processes to ensure completion of all ISAs as required for their ministry in accordance with the ISA Directions and section 69 of FOIPPA.

2.6.9 MPOs must develop, maintain and review internal processes to ensure completion of all CPAs or IPAs when a CPA or IPA is identified as being required for their ministry in accordance with section 69 of FOIPPA and section 12 of the FOIPP Regulation.

2.6.10 MPOs must develop, maintain and review internal processes to ensure completion of all RAs as required for their ministry in accordance with section 33(3)(h)(v) of FOIPPA.

2.6.11 MPOs must ensure any ISAs, RAs, CPAs and IPAs are updated when they are made aware of substantive changes to an initiative.

2.6.12 MPOs must report all completed ISAs, including IPAs and CPAs, to CIRMO for entry into the PID and must do so in the manner and form as directed by CIRMO.

2.6.13 MPOs must keep an inventory of all RAs entered into by their ministry.

2.6.14 An MPO may be granted an exemption for accountabilities in s.2.6 at the discretion of CIRMO and determined on a case-by-case basis. An exemption does not prevent an MPO from remaining involved. For an exemption to be granted, the re-allocation of roles and responsibilities must be documented in the manner and form directed by CIRMO.

Corporate Information and Records Management Office

2.6.15 CIRMO is responsible for issuing exemptions to the requirement to enter into an ISA in accordance with the ISA Directions.

2.7 Personal Information Directory

Ministry Privacy Officers

2.7.1 MPOs must report to CIRMO for entry into the PID any Personal Information Banks (PIBs) that result from new systems, projects, programs, or activities of a ministry, in the manner and form as directed by CIRMO. Note that PIBs are often reported through a PIA.

2.7.2 MPOs must ensure the information contained in the PID for their respective ministry is accurate, in accordance with section 69(4) of FOIPPA, and updated as needed.

2.7.3 The MPO for the Ministry of Health must ensure that the required information regarding Health Information Banks (HIBs) is submitted to CIRMO for entry into the PID.

Corporate Information and Records Management Office

2.7.4 CIRMO must manage and publish the PID monthly. This includes revising entries with updated information provided by the MPOs and notifying MPOs when the PID has been published.

2.8 Information Management Practice Reviews

Ministry Privacy Officers

2.8.1 MPOs must complete reviews of their privacy management practices.

2.9 Information Incident Management

Employees

2.9.1 Employees must immediately report actual or suspected information incidents, including Privacy Breaches and privacy complaints, in accordance with the Information Incident Management Policy. Please refer to the Information Incident Management Policy for more information on the requirements for responding to Information Incidents, including Privacy Breaches.

2.10 Service Provider Management

Employees

2.10.1 Employees who prepare or manage contracts must include the Privacy Protection Schedule or the Privacy Protection Schedule for Cloud Services in all contracts that involve Personal Information in the custody or under the control of the public body, except where an alternative version is approved by CIRMO.

2.10.2 Employees must submit any alternative terms for the Privacy Protection Schedule or Privacy Protection Schedule for Cloud Services to CIRMO for approval prior to the execution of the related contract.

2.10.3 Where Personal Information is in the custody or under the control of a ministry, Employees who prepare or manage contracts must inform MPOs of all Service Providers and volunteers whose contracts involve the access, collection or creation of Personal Information to enable MPOs to meet the requirements set out in s.2.4.6.

Corporate Information and Records Management Office

2.10.4 CIRMO must review any alternative versions of the terms for the Privacy Protection Schedule or Privacy Protection Schedule for Cloud Services that are submitted to CIRMO for authorization in accordance with Chapter 6 of Core Policy and the Procurement Practice Standard.

Appendix A – Glossary

Common or Integrated Program or Activity (as defined in FOIPPA, Schedule 1) means a program or activity that

(a) provides one or more services through
(i) a public body and one or more other public bodies or agencies working collaboratively; or
(ii) one public body working on behalf of one or more other public bodies or agencies; and
(b) is confirmed by regulation as being a common or integrated program or activity.

Contact Information (as defined in FOIPPA, Schedule 1) means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

Employee means an individual working for the Government of British Columbia and includes Service Providers and volunteers.

FOIPPA Delegation Instrument means the tool by which the head of a public body authorizes an Employee within the public body or another public body to exercise one or more of the head's authorities or decision-making powers under FOIPPA. The person delegating the authority remains responsible and accountable for all actions and decisions made under that delegation.

Health Information Bank (as defined in FOIPPA, section 69.1(1)) means a health information bank and a ministry database within the meaning of the E-Health (Personal Health Information Access and Protection of Privacy) Act.

Information Incident means a single or a series of events involving the collection, storage, access, use, disclosure, or disposal of government information that threaten privacy or information security and/or contravene law or policy.

Information-Sharing Agreement is an agreement that sets conditions on the collection, use or disclosure of Personal Information by the parties to the agreement. It is an agreement between a public body and one or more of the following (as defined in FOIPPA S 69(1)):

(a) another public body;
(b) a government institution subject to the Privacy Act (Canada);
(c) an organization subject to the Personal Information Protection Act or the Personal Information Protection and Electronics Documents Act (Canada);
(d) a public body, government institution or institution as defined in applicable provincial legislation having the same effect as FOIPPA;
(e) a person or group of persons; or
(f) an entity prescribed in the FOIPP Regulation.

Ministry Privacy Officer means the designated individual in each ministry accountable for privacy and the implementation of this policy within their ministry.

Personal Information (as defined in FOIPPA, Schedule 1) means recorded information about an identifiable individual other than contact information.

Personal Information Bank (as defined in FOIPPA, section 69(1)) means an aggregation of Personal Information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

Personal Information Directory means the public-facing database used to document the management of Personal Information holdings of government and to assist the public in identifying the location of Personal Information about them held by government.

Supplementary Assessment refers to additional considerations in the PIA when public bodies are contemplating disclosing sensitive personal information to be stored outside of Canada in accordance with the Personal Information Disclosure for Storage Outside of Canada Regulation.

Privacy Breach means the theft or loss, or the collection, use or disclosure of Personal Information that is not authorized by Part 3 of FOIPPA. A Privacy Breach is a type of Information Incident.

Privacy Impact Assessment (as defined in FOIPPA, section 69(1)) means 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 (Protection of Privacy) of FOIPPA.

Privacy Protection Schedule (or Privacy Protection Schedule for Cloud Services) means the schedule completed and attached to any contract between the government and a Service Provider that involves Personal Information. Its purpose is to: (a) enable the Province to comply with its statutory obligations under FOIPPA with respect to Personal Information; and (b) ensure that the Service Provider is aware of and complies with its statutory obligations under FOIPPA with respect to Personal Information.

Research Agreement means an agreement setting out the approved conditions under which Personal Information is disclosed for research purposes in accordance with s.33(3)(h) of FOIPPA.

Service Provider (as defined in FOIPPA, Schedule 1) means a person retained under contract to perform services for the Government of British Columbia.

Appendix B – Links to Key Resources

Appropriate Use Policy

Core Policy and Procedures Manual (CPPM) Policy Chapter 6: Procurement

Core Policy and Procedures Manual (CPPM) Policy Chapter 12: Information Management and Information Technology Management

Freedom of Information and Protection of Privacy Act (FOIPPA)

Freedom of Information and Protection of Privacy Regulation

FOIPPA Delegation Instrument

FOIPPA Foundations Training

Guidance on Disclosures Outside of Canada

Information Incident Management Policy

Information Sharing Agreements: Directions, Template and Guidance

Managing Government Information Policy

Ministry Privacy Officer Directory

Personal Information Directory (via the Data Catalogue)

Personal Information Disclosure for the Storage Outside of Canada Regulation

Privacy Impact Assessments: Directions

Privacy Impact Assessments: Guidance

Privacy Impact Assessments: Template

Privacy Protection Schedules

Sample Research Agreement Form

Training Resources

For questions, contact the Privacy & Access Helpline:
Telephone: +1-250-356-1851
Email: privacy.helpline@gov.bc.ca