Privacy Management and Accountability Policy

Corporate Information and Records Management Office
Privacy, Compliance and Training Branch
Ministry of Citizens' Services

Version 3.0

BRITISH COLUMBIA

Table of Contents

1.0 Introduction

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 must be followed by ministries. All these measures work together to support compliance with FOIPPA.

PMAP articulates the privacy related requirements of all employees working for ministries within the Province of British Columbia. As defined by FOIPPA, a public body's "employee" includes both volunteers and service providers. In addition to their responsibilities as employees, PMAP outlines the specific accountabilities of Deputy Ministers, Ministry Privacy Officers (MPOs), and the Corporate Information and Records Management Office (CIRMO) on matters related to privacy. Deputy Ministers are responsible for supporting the continuous improvement of privacy practices and the responsible collection, use, disclosure, storage, access, retention and destruction of personal information in their ministry. Deputy Ministers are also responsible for ensuring that PMAP is communicated to all employees in their respective ministry.

The Privacy, Compliance and Training Branch (PCT) in CIRMO within the Office of the Chief Information Officer (OCIO) is BC 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 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 accountable stewards of personal information and PMAP helps to support the expansion of positive privacy practices within each ministry. Positive privacy practices enable employees to demonstrate accountability and enhance services to citizens.

1.1 Scope

PMAP applies to all ministries in the Province of B.C.

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 the Core Policy and Procedures Manual.

1.4 Legal Considerations

FOIPPA protects personal privacy by prohibiting the unauthorized collection, use, disclosure, storage and destruction of personal information by government ministries and other public bodies. PMAP does not replace or limit a ministry's obligations under FOIPPA; 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 B.C.'s central privacy office. Advice on PMAP can be obtained from 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 the Corporate Information and Records Management Office (CIRMO) within the Office of the Chief Information Office (OCIO). This individual will be designated the Ministry Privacy Officer (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 B.C. (e.g. Public Service Agency, Government Communications and Public Engagement).

Ministry Privacy Officers

2.1.2 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 have delegated.

2.1.3 MPOs may develop ministry specific policies and procedures to support this policy or compliance with the Freedom of Information and Protection of Privacy Act (FOIPPA). Any such ministry specific policies must be submitted to CIRMO for review during development of the policies.

2.1.4 MPOs must communicate substantive changes to the Privacy Management and Accountability Policy (PMAP) to relevant ministry employees.

Corporate Information and Records Management Office

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

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

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

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

2.1.9 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 updated copies to CIRMO.

Corporate Information and Records Management Office

2.3.3 CIRMO will 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 destruction of personal information as prescribed by CIRMO, i.e. the IM117 course offered through the Public Service Agency. An exemption may be granted in extenuating circumstances by CIRMO.

2.4.2 Employees must complete the ministry specific training or awareness activities referenced in s.2.4.6 and s.2.4.7, when applicable.

2.4.3 Employees who are service providers and/or volunteers who collect or create personal information must complete privacy training developed by CIRMO on the appropriate collection, use, disclosure, storage, access, retention and destruction of personal information, unless granted an exemption by CIRMO. 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).

Ministry Privacy Officers

2.4.4 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.

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

i. 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.

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

2.4.7 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 the privacy obligations. MPOs may use resources developed in collaboration with CIRMO or may use tools developed by CIRMO (once made available).

2.4.8 Once Ministry-specific training or awareness activities referred to in s.2.4.6 and/or s.2.4.7 are developed, MPOs must ensure that the required activities are completed by all appropriate employees within a timeline as determined by the MPO.

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.

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, and then the PIA must be submitted to CIRMO for review and comment. PIAs must be completed during the development of the proposed enactment, system, project, program or activity. 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 the mitigation strategies identified in the risk mitigation table of the PIA with the support of their MPO (see s.2.5.8).

2.5.5 As stated in s.2.5.11 under certain circumstances, at the discretion of CIRMO, employees may work directly with Privacy, Compliance and Training Branch (PCT) instead of their MPO. Such cases will be examined on a case-by-case basis and in consultation with the MPO.

Ministry Privacy Officers

2.5.6 MPOs must develop, maintain and review internal processes to ensure that that PIAs are completed. 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. PIAs must be completed during the development of any new or updated enactment, system, project, program or activity.

2.5.7 MPOs must develop, maintain and review internal processes to ensure the mitigation of risks identified in the risk mitigation table in PIAs, within their ministry.

2.5.8 MPOs must support program areas, where necessary, in the reasonable implementation of mitigation strategies identified in the risk mitigation table of the PIA.

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

Corporate Records and Information Management Office

2.5.10 CIRMO must review and comment on all PIAs submitted by ministries.

2.5.11 There may be exceptions to the MPO accountabilities in s.2.5, determined at the discretion of CIRMO on a case-by-case basis, in consultation with the MPO, and in accordance with the PIA Directions and FOIPPA. These circumstances do not preclude an MPO from remaining involved.

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.

2.6.2 Employees must complete Research Agreements (RAs) in accordance with section 35 of FOIPPA.

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

2.6.4 Employees must consult their MPO (or other role identified as per 2.6.13) before entering into an ISA with a private sector organization outside of a contractual relationship.

2.6.5 Employees must notify the MPO of all completed ISAs, IPAs and CPAs, to CIRMO for entry into the PID and do so in the manner and form as directed by CIRMO.

2.6.6 Employees must notify the MPO when there are any substantive changes to an ISA, RA, CPA, IPA.

Ministry Privacy Officers

2.6.7 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.

2.6.8 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.

2.6.9 MPOs must develop, maintain and review internal processes to ensure completion of all RAs as required for their ministry in accordance with section 35 of FOIPPA.

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

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

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

2.6.13 An MPO may be granted an exemption for accountabilities in s.2.6, at the discretion of CIRMO, determined on a case-by-case basis. An exemption does not preclude 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 Records and Information Management Office

2.6.14 CIRMO is responsible for issuing exemptions to the requirement to enter into an ISA, as per the ISA Directions.

2.7 Personal Information Inventories and Directory

Ministry Privacy Officers

2.7.1 MPOs must develop, maintain, and review internal processes to ensure that their ministry's personal information holdings and any other required details are listed in a Personal Information Inventory in accordance with the Personal Information Inventory Policy (once issued).

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

2.7.3 MPOs must ensure the information contained in the PID for their respective ministry is accurate in accordance section 69(4) of FOIPPA and updated as needed. This requires, at minimum, an annual check for accuracy in accordance with Core Policy.

2.7.4 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

2.7.5 CIRMO must consult with MPOs and recommend a mechanism for ministries to document details of their personal information holdings as required by the Personal Information Inventory Policy (once issued).

2.7.6 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 in accordance with the Information Management Practice Review Policy. Please refer to the Information Management Practice Review Policy (once issued) for more information regarding practice reviews.

2.9 Information Incident Management

Employees

2.9.1 Employees must immediately report actual or suspected Information Incidents, including privacy breaches and privacy complaints as per 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 Foreign Demands for Disclosure

Employees

2.10.1 Employees receiving Foreign Demands for Disclosure must immediately notify CIRMO. Notice may be provided in the form provided by CIRMO.

2.10.2 CIRMO must inform the MPO when a Foreign Demand for Disclosure for their ministry has been received, when relevant.

Corporate Information and Records Management Office

2.10.3 CIRMO will brief the Minister responsible for FOIPPA in accordance with section 30.2 of FOIPPA.

2.11 Service Provider Management

Employees

2.11.1 Employees who prepare or manage contracts must include the Privacy Protection Schedule in all contracts that involve personal information in the custody or under the control of the public body, except where an alternate version is approved by CIRMO.

2.11.2 Where personal information is in the custody or control of a ministry, employees who prepare or manage contracts must inform MPOs of all service providers and volunteers that collect or create personal information or where personal information is accessible to them to enable MPOs to meet the requirements set out in s.2.4.4.

Corporate Information and Records Management Office

2.11.3 CIRMO must review any alternate versions of the Privacy Protection Schedule that are submitted to CIRMO for authorization as per Core Policy.

Appendix A – Glossary

Common or Integrated Program or Activity 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 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.

Foreign Demand for Disclosure means a subpoena, warrant, order, demand or request that is

(a) from a foreign court, an agency of a foreign state or another authority outside Canada, and
(b) for the unauthorized disclosure of personal information to which FOIPPA applies.

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 means an agreement between a public body and one or more of the following:

(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 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

that sets conditions on the collection, use or disclosure of personal information by the parties to the agreement.

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

Personal Information means recorded information about an identifiable individual other than contact information.

Personal Information Bank means a collection 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.

Personal Information Inventory means a listing of all personal information holdings held by a ministry.

Privacy Breach means the collection, storage, access, use, disclosure, or disposal of personal information that is not authorized by Part 3 of the *Freedom of Information and Protection of Privacy Act*. A privacy breach is a type of information incident.

Privacy Impact Assessment 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 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, pursuant to s.35 of FOIPPA.

Service Provider means a person retained under contract to perform services for the Government of British Columbia.

Unauthorized Disclosure of Personal Information means disclosure of, production of or the provision of access to personal information to which FOIPPA applies, if that disclosure, production or access is not authorized by FOIPPA.

Appendix B – Links to Key Resources

Core Policy and Procedures Manual (CPPM) Policy Chapter 12: Information Management and Information Technology Management
https://www2.gov.bc.ca/gov/content/governments/policies-for-government/core-policy/policies/im- it-management

Core Policy and Procedures Manual (CPPM) Policy Chapter 6: Procurement: https://www2.gov.bc.ca/gov/content/governments/policies-for- government/core-policy/policies/procurement

Freedom of Information and Protection of Privacy Act (FOIPPA):
http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00

FOIPPA Delegation Instrument:
https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services- policies-for-government/information-management-technology/information-privacy/resources/templates/foippa_delegation_instrument.docx

Freedom of Information and Protection of Privacy Regulation:
http://www.bclaws.ca/civix/document/id/complete/statreg/155_2012

Foreign Demand for Disclosure Form:
https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services- policies-for-government/information-management-technology/information-privacy/resources/policies-guidelines/foreign_demand_for_disclosure_form_-_fillable_pdf.pdf

Information Incident Management Policy:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information- management-technology/privacy/privacy-breaches

ISA Directions:
http://www.bclaws.ca/civix/document/id/mo/mo/2019_m327

ISA Template:
https://www2.gov.bc.ca/gov/content/governments/services-for-government/information- management-technology/privacy/agreements-contracts

Ministry Privacy Officer Directory:
www.gov.bc.ca/privacyofficers

Personal Information Directory (via DataBC):
http://catalogue.data.gov.bc.ca/dataset/bc-personal-information-directory-pid

Personal Information Inventory Policy:
Under development

Information Management Practice Review Policy:
Under development

Privacy Impact Assessment Directions, Template and Guidelines:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information- management-technology/privacy/privacy-impact-assessments

Privacy Protection Schedule:
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information- management-technology/privacy/agreements-contracts/privacy-protection-schedule

Sample Research Agreement Form:
http://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies- for-government/information-management-technology/information- privacy/resources/templates/research-agreement-sample.pdf

Training Resources:
To learn about training opportunities on PIAs, Privacy Governance, contact Privacy & Access Helpline. https://www2.gov.bc.ca/gov/content/governments/services- for-government/information-management-technology/privacy/training