Privacy Management and Accountability Policy

Corporate Information and Records Management Office
Privacy, Compliance and Training Branch
Ministry of Finance

BRITISH COLUMBIA

Version 1.1
May 2016

Directive to Ministries from the Government Chief Records Officer:

The Government of British Columbia continually strives to enhance its interactions with citizens by pushing boundaries and setting new standards for service delivery in B.C. The use of new technology to simplify service delivery often results in an improved ability for government to synthesize information to provide a foundation for government's decision-making, policy development and future service delivery improvements. Some of this information can be very sensitive personal information, and as such must be collected, used, disclosed, stored and destroyed with due care. Government must be diligent in ensuring that correct processes are in place to protect personal information and to use it in a privacy-enhancing manner.

As the Government Chief Records Officer, I am responsible for setting the corporate direction and policy with respect to information management, in a manner consistent with the broader direction of government and the Minister of Finance. This includes direction and policy to protect the privacy of the personal information that is entrusted to government. The purpose of this Directive is twofold: to establish a new corporate privacy policy — the Privacy Management and Accountability Policy (PMAP) — and to inform ministries about their obligation to promote and support compliance with the provisions of this policy.

The PMAP sets out specific requirements for privacy in the areas of accountability for privacy management; education and awareness; privacy impact assessments; agreements involving the sharing of personal information; personal information inventories and directories; privacy breach and information incident management; foreign demands for disclosure; Service Provider management; and compliance reviews and audits. Specific roles and responsibilities for ministries, my office, and Employees are also established in order to provide clear guidance on who is responsible for fulfilling these policy requirements. In addition, ministries are required to demonstrate compliance with this policy.

As digital information becomes the norm for government in all of its evaluation and decision-making processes it has become even more important for all ministries to demonstrate their compliance with the *Freedom of Information and Protection of Privacy Act* (FOIPPA), but also to go beyond that and to incorporate privacy into their daily activities. The PMAP is designed to ensure compliance but also foster an important culture of privacy within government as a whole.

Signed February 4, 2016:

Cheryl Wenezenki-Yolland,
Associate Deputy Minister and Government Chief Records Officer

BRITISH COLUMBIA | Ministry of Finance

Document Purpose and Objectives

The Privacy Management and Accountability Policy (PMAP) is government's corporate approach to privacy management. The PMAP acts as the framework under which all ministries must operate in order to ensure that the government of B.C. is compliant with the privacy requirements of the *Freedom of Information and Protection of Privacy Act* (FOIPPA), and manages its personal information holdings in the most efficient manner.

The PMAP clarifies the privacy management roles and responsibilities of Government's ministries, the Corporate Information and Records Management Office (CIRMO) and Employees. The Privacy, Compliance and Training Branch within the CIRMO is government's central privacy office.

The PMAP identifies the mandatory assessment tools and agreements that must be completed by ministries, as well as reporting and audit requirements. The PMAP identifies the policies and procedures that must be followed by ministries to ensure compliance with the privacy provisions of FOIPPA.

Specifically, the objective of the PMAP is to clearly articulate and provide direction regarding:

- Accountability for privacy management requirements;
- development, completion and review of ministry-specific privacy policies that ensure the lawful collection, use, disclosure, storage and destruction of personal information;
- development, completion and review of privacy impact assessments;
- development, completion and review of Information Sharing Agreements, Research Agreements, and Common or Integrated Program or Activity Agreements;
- management of the Personal Information Directory;
- management of Privacy Breaches and complaints;
- development, completion and review of compliance and auditing tools and processes; and
- ongoing employee privacy awareness and education, including specific awareness and education for Service Providers.

Advice on this Policy

Advice on the PMAP can be obtained from:

Privacy, Compliance and Training Branch
Corporate Information and Records Management Office
Ministry of Finance
Telephone: 250-356-0361
Facsimile: 250-356-1182
Web: http://gov.bc.ca/privacypolicy

Revision History

Date	Revisions	Author
February 4, 2016	Version 1.0	Privacy, Compliance and Training Branch
May 13, 2016	Update to broken links; Amendment to ensure contractor training requirements reflect the Privacy Protection Schedule; Minor amendments made to ensure consistency between PMAP Policy Requirements and Roles and Responsibilities.	Privacy, Compliance and Training Branch

Table of Contents

1.0 Introduction

The *Freedom of Information and Protection of Privacy Act* (FOIPPA) protects the personal privacy of B.C. citizens by prohibiting the unauthorized collection, use, or disclosure of personal information by public bodies.

The Privacy Management and Accountability Policy (PMAP) sets the framework for privacy to be a central component of all government's business practices and a built-in component of day-to-day program operations. The PMAP strengthens government's ability to protect the privacy of citizens' personal information by clearly articulating key privacy policies and roles and responsibilities for privacy management within government.

1.1 Scope

The PMAP applies to all government ministries.

1.2 Effect

The requirements and accountabilities of this policy take effect immediately upon publication of the policy, with the exception of requirements related to Personal Information Inventories and Compliance Reviews and Audits, where relevant policies or guidelines are not yet in place. When published, the related policies and guidelines will set out relevant effective dates.

Specifically, the following sections will not be in effect until further notice or publication:

- 2.5.1
- 2.5.2
- 2.9.2

1.3 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. It is important to note that the PMAP does not replace or limit a ministry's obligations under FOIPPA; rather the PMAP supports compliance with the privacy requirements of the Act. Ministries must ensure they meet all of their obligations under FOIPPA.

1.4 Terms and Definitions

The following definitions are provided for key terms and acronyms used in this document. Links to key documents are also provided here or can be found in "Appendix A – Websites".

Common or Integrated Program or Activity	"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 (iii) is confirmed by regulation as being a common or integrated program or activity.
Common or Integrated Program or Activity Agreement (IPA)	"Common or Integrated Program or Activity Agreement" means the agreement that confirms that a program or activity is a common or integrated program or activity pursuant to s.12 of the FOIPP Regulation. Where this agreement fulfills the definition of an "**Information Sharing Agreement**" requirements for ISAs apply.
Employee	"Employee" means an individual working for the Government of British Columbia, including Service Providers or volunteers.
FOIPPA Delegation Instrument	"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	"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	"Information Incident" means a single or a series of unwanted or unexpected events that threaten privacy or information security, including a Privacy Breach or the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by the

	business owner of that information.
Information Sharing Agreement (ISA)	"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 (MPO)	"Ministry Privacy Officer" means the designated individual from each ministry responsible for privacy and the

	implementation of this policy within their ministry.
Personal Information Directory (PID)	"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	"Personal Information Inventory" means a listing of all personal information holdings held by a ministry.
Privacy Breach	"Privacy Breach" means a type of information incident where there is a collection of, use of, disclosure of, access to, disposal of, or storage of personal information, whether accidental or deliberate, that is not authorized by FOIPPA.
Privacy Impact Assessment (PIA)	"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 Management and Accountability Policy (PMAP) Delegation Instrument	"PMAP Delegation Instrument" means the tool by which an Employee authorizes another Employee within the public body or another public body to exercise one or more of their authorities or decision-making powers under this policy. The person delegating the authority remains responsible and accountable for all actions and decisions made under that delegation.
Privacy Protection Schedule	"Privacy Protection Schedule" means a 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	"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	"Service Provider" means a person retained under contract to perform services for the Government of British Columbia.
Unauthorized Disclosure of Personal Information	"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.

2.0 Policy Requirements

2.1 Accountability for Privacy Management

2.1.1 Deputy Ministers must ensure that the Privacy Management and Accountability Policy (PMAP) is communicated to all Employees in their respective ministry.

2.1.2 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). This individual will be designated the Ministry Privacy Officer (MPO).

2.1.3 MPOs may delegate any roles and responsibilities assigned to them under the PMAP but remain accountable as the single point of contact for the CIRMO.

2.1.4 Employees must comply with the PMAP and other privacy-related policies, guidelines and templates developed by the CIRMO.

2.1.5 MPOs must coordinate and manage their ministry's compliance with the PMAP and any corporate directions, policies, guidelines and templates that flow from the PMAP.

2.1.6 Deputy Ministers must use a FOIPPA Delegation Instrument if they wish to delegate any duties, powers or functions of the head under FOIPPA to the MPO, any other Employees of the ministry or another public body. The Deputy Minister may perform this duty as head of the public body as per section 23 of the *Interpretation Act*.

2.1.7 MPOs must maintain any current FOIPPA Delegation Instruments for their ministry, and provide updated copies to the CIRMO.

2.1.8 The MPO must develop in collaboration with the CIRMO, issue, and maintain ministry-specific privacy policies where necessary, to support the PMAP.

2.1.9 The CIRMO must

(a) Review the PMAP annually with input from MPOs and update as appropriate and

(b) Inform MPOs of all significant changes to the PMAP.

2.1.10 The MPO must communicate any significant changes to the PMAP to their ministry Employees.

2.1.11 The CIRMO must establish and chair a Privacy Management Community of Practice to facilitate dialogue between the MPOs, the CIRMO, and other interested parties.

2.1.12 Employees must engage with the CIRMO before contacting the Office of the Information and Privacy Commissioner on matters relating to privacy.

2.2 Education and Awareness

2.2.1 Employees must complete training relevant to their job on the appropriate collection, use, disclosure, storage and destruction of personal information as prescribed by the CIRMO. This includes the following requirements:

- for all Employees: training on FOIPPA and privacy generally, including the appropriate collection, use,

disclosure, storage and destruction of personal information (the IM111 course offered through the Public Service Agency may be applied towards this requirement)

- For any Employees whose work function requires it: training on Privacy Impact Assessments and Information Sharing Agreements.

2.2.2 All Employees who are Service Providers and/or volunteers who collect or create personal information must complete training on the appropriate collection, use, disclosure, storage and destruction of personal information as prescribed by the CIRMO here. This training must be completed prior to providing any service that involves personal information. Training referred to in s.2.2.1 may be applied towards this requirement (where it has been documented).

2.2.3 MPOs must develop, in collaboration with the CIRMO, Ministry-specific training related to information systems and programs that involve the handling of high-risk or sensitive personal information within their ministry.

2.2.4 MPOs must ensure that mandatory training referred to in s.2.2.1, and 2.2.2 is taken by all Employees, as applicable.

2.2.5 MPOS must ensure that a process is in place for communicating notice of changes regarding access to Personal Information by Service Providers and volunteers so that training requirements can be properly applied.

2.2.6 Once Ministry-specific training referred to in s.2.2.3 is developed, MPOs must ensure that the training is completed by all appropriate Employees within 6 months of working with an information system or program that involve the handling of high-risk or sensitive personal information.

2.3 Privacy Impact Assessments

2.3.1 Employees must conduct Privacy Impact Assessments (PIA) in accordance with the PIA Directions as issued by the Minister responsible for FOIPPA, and must use the templates developed by the CIRMO.

2.3.2 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.

2.3.3 MPOs must ensure PIAs are completed where necessary, and review PIAs before submission to the CIRMO for review and comment.

2.3.4 After the MPO completes their review, Employees must submit PIAs to the CIRMO for review and comment. A PIA is not complete until it has been fully signed by all required parties as set out in the PIA Directions. PIAs must be completed before the start of the proposed enactment, system, project, program, or activity.

2.3.5 Any PIA signatory authorized by the PIA Directions may delegate their authority to sign PIAs using a PMAP Delegation Instrument.

2.3.6 MPOs must maintain any current PMAP Delegation Instruments for their ministry, and provide updated copies to the CIRMO.

2.3.7 MPOs must ensure that a copy of each completed and signed PIA is provided to the CIRMO for retention and for entry into the Personal Information Directory (PID), and once drafted, must do so in accordance with the PID Policy (currently being drafted).

2.3.8 MPOs must develop, maintain and review internal processes to ensure completion of accurate PIAs within their ministry.

2.4 Agreements

2.4.1 Once drafted, Employees must prepare Information Sharing Agreements (ISA) in accordance with the ISA Directions (currently being drafted).

2.4.2 Employees must complete ISAs using the template developed by the CIRMO, unless granted an exemption by the CIRMO. An ISA is not complete until it has been fully signed by all required parties as set out in the ISA Directions.

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

2.4.4 Employees must complete Common or Integrated Program or Activity Agreements (IPAs) in accordance with section 12 of the FOIPP Regulation.

2.4.5 Employees must conduct a PIA for each ISA or IPA developed.

2.4.6 MPOs must ensure completion of, and conduct review of all:

- ISAs,
- RAs, and
- IPAs

required in their ministry.

2.4.7 MPOs must ensure any ISAs, RAs, and IPAs are updated when changes are made to an initiative.

2.4.8 MPOs must develop, maintain and review internal processes to ensure completion of accurate ISAs, RAs, and IPAs within their ministry.

2.4.9 MPOs must report all completed ISAs to the CIRMO for entry into the PID, and once drafted, must do so in accordance with the PID Policy (currently being drafted).

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

2.5 Personal Information Inventories and Directory

2.5.1 The CIRMO must work collaboratively with ministries to establish a mechanism for ministries to document details of their personal information holdings as required by the Personal Information Inventory Policy (currently being drafted).

2.5.2 MPOs must ensure that their ministry's personal information holdings and other details as listed in the Personal Information Inventory Policy (currently being drafted) are listed in a Personal Information Inventory within one year of the Personal Information Inventory Policy being published.

2.5.3 MPOs must report Personal Information Banks (PIB) that result from new enactments, systems, projects, programs, or activities of a ministry to the CIRMO for entry into the PID,

and once drafted, must do so in accordance with the PID Policy (currently being drafted).

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

2.6 Information Incident Management

2.6.1 Employees must immediately report actual or suspected Privacy Breaches, including privacy complaints as per the Information Incident Management Policy.

2.6.2 The CIRMO must coordinate, investigate and resolve all Privacy Breaches and complaints in accordance with the Information Incident Management Policy.

2.6.3 Employees must follow all instructions and recommendations issued by the CIRMO during an information incident investigation.

2.6.4 MPOs must provide the CIRMO, as required, timelines and follow-up reports on steps taken to ensure implementation of and compliance with recommendations made after a Privacy Breach investigation.

2.6.5 The CIRMO may conduct compliance reviews to assess ministry compliance with CIRMO instructions and recommendations issued during an information incident investigation.

2.6.6 The CIRMO must maintain and monitor a means for ministries to report information incidents 24-hours per day, 365 days per year.

2.6.7 The CIRMO must maintain and monitor for government a public telephone number where citizens can make a privacy complaint directly.

2.7 Foreign Demands for Disclosure

2.7.1 Employees receiving Foreign Demands for Disclosure must immediately notify the CIRMO in the manner and form directed by the CIRMO.

2.8 Service Provider Management

2.8.1 Employees who prepare or manage contracts must include the standard 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 the CIRMO.

2.8.2 Employees who prepare or manage contracts must inform MPOs of all Service Providers and volunteers that have access to personal information within the ministry's custody and control.

2.8.3 MPOs must ensure that Service Providers and volunteers referred to in section 2.2.2 complete the relevant training.

2.9 Compliance Reviews and Audits

2.9.1 The CIRMO may conduct compliance reviews in order to assess compliance with FOIPPA and this policy, and once drafted, must do so in accordance with the Privacy Compliance Audit Policy.

2.9.2 MPOs must conduct self-audits and communicate results to the CIRMO as per the Privacy Compliance Audit Policy (once drafted).

2.9.3 MPOs must assist the CIRMO with any compliance review of their ministry's privacy management practices, where necessary.

2.9.4 MPOs must ensure necessary information is recorded and retained in support of any future compliance review or audit.

3.0 Roles and Responsibilities for Privacy Management

The Corporate Information and Records Management Office has the responsibility to:

Accountability for Privacy Management:

- Maintain the PMAP and review annually
- Consult with MPOs when reviewing the PMAP
- Inform MPOs of all significant changes to the PMAP
- Provide advice regarding the PMAP
- Develop, issue, and update corporate directions, policies, guidelines, and templates that provide further direction or clarification on any provision of the PMAP
- Maintain metrics on privacy management program compliance and report out to ministries through the respective MPO
- Provide support to ministries on the development of ministry-specific privacy policies
- Provide orientation for new MPOs regarding their role and responsibilities under the PMAP
- Provide support to MPOs to ensure compliance with the PMAP within individual ministries
- Keep a record of all current FOIPPA and PMAP Delegation Instruments for each Ministry
- Provide support to ministries in all discussions with the Office of the Information and Privacy Commissioner (OIPC)
- Establish and chair a Privacy Management Community of Practice

Education & Awareness:

- Develop and make available to all Employees training on each of the following topics:
  - FOIPPA (including how to appropriately collect, use, disclose, store and destroy personal information)
  - Privacy Impact Assessments and Information Sharing Agreements
  - Privacy and Information Sharing Awareness
  - Dedicated training where a need has been identified as part of the resolution of a Privacy Breach
- Provide a comprehensive certificate based training program on:
  - Privacy governance;
  - Security
  - Access to information and records management;
  - Privacy Breach management;
  - Privacy compliance tools; and
  - Additional topics of relevance

- Develop and deliver training for Service Providers and volunteers

PIAs, Agreements, Inventories and the PID:

- Maintain the PIA and ISA Directions and other guideline documents
- Review and comment on PIAs submitted by ministries
- Update the PID with information provided by ministries
- Work collaboratively with ministries to create a corporate means for ministries to document their personal information holdings
- Consult with the OIPC when appropriate

Privacy Breaches and Information Incidents:

- Maintain and update the Information Incident Management Policy as necessary
- Investigate, coordinate, and resolve investigations into privacy incidents and complaints
- Inform MPOs of information incidents received for their ministry and work collaboratively with them to resolve any incidents
- Conduct compliance reviews to ensure compliance with CIRMO instructions and recommendations made to program areas during Privacy Breach investigations
- Consult with the OIPC when appropriate
- Maintain and monitor a 24 hour breach reporting instrument
- Maintain and monitor a public telephone number for citizens to make privacy complaints

Compliance Reviews and Audits:

- Develop, maintain and update audit template and policy as necessary
- Review audits submitted by MPOs and provide assistance where necessary
- Conduct compliance reviews as per the Privacy Compliance Audit Policy

Deputy Ministers have the responsibility to:

Accountability for Privacy Management:

- Ensure that the PMAP is communicated to all Employees within their ministry
- Lead their ministry to create an enhanced culture of privacy and the responsible collection, use, disclosure, storage and destruction of personal information
- Promote the value of meeting the requirements of the PMAP
- Encourage MPOS to consider the objectives of the PMAP in all circumstances where the ministry collects, uses, discloses, stores or destroys personal information

- Designate a MPO and provide their contact information to the CIRMO
- Complete the FOIPPA Delegation Instrument, as required, to delegate any duties, powers or functions of the head under FOIPPA to the MPO or any other Employees of the Ministry or another public body

The **Ministry Privacy Officer** has the responsibility to:

Accountability for Privacy Management:

- Support their ministry in maintaining an enhanced culture of privacy and the responsible collection, use, disclosure, storage and destruction of personal information
- Coordinate and manage their ministry's compliance with the PMAP, and any corporate directions, policies, guidelines, and templates that flow from the PMAP
- Act as the single point of contact for the CIRMO regarding the ministry's compliance with the PMAP
- Where necessary, develop, issue, and maintain ministry specific privacy policies in collaboration with the CIRMO
- Submit their ministry's current FOIPPA Delegation Instrument and any PMAP Delegation Instruments to the CIRMO
- Communicate any significant changes to the PMAP to their ministry's Employees
- Consider the objectives of the PMAP in all circumstances where the ministry collects, uses, discloses, stores or destroys personal information

PIAs, Agreements, Inventories and the PID:

- Develop, maintain and review internal processes to ensure the completion of accurate PIAs, ISAs, RAs and IPAs within their ministry
- Review all PIAs before they are submitted to the CIRMO for review
- Review and comment on all RAs, IPAs and ISAs
- Ensure PIAs, ISAs, RAs and IPAs are updated when changes are made to an initiative
- Maintain a personal information inventory for their respective ministry, in accordance with Personal Information Inventory Policy
- Ensure that a final signed PIA is submitted to the CIRMO to enter into the PID
- Notify the CIRMO of any required updates or changes to their ministry's ISA and PIB entries in the PID as per the PID Policy
- Inform the CIRMO of any changes to the status of items listed on the PID
- Ensure that the required information regarding HIBs is submitted to the CIRMO for entry into the PID, as applicable to the Ministry Privacy Officer for the Ministry of Health

- Keep an inventory of all RAs entered into by their ministry

Education & Awareness:

- Ensure that all new Employees receive training within the first year of their employment on:
    - FOIPPA or privacy generally, including the appropriate collection, use, disclosure, storage and destruction of personal information (the IM111 course offered through the Public Service Agency may be applied towards this requirement)
    - Privacy Impact Assessments and Information Sharing Agreements (where appropriate to their work function)
- Develop ministry-specific training in collaboration with the CIRMO and deliver to Employees, as applicable
- Provide refresher courses on ministry-specific training on an ongoing basis
- Ensure that all Service Providers and volunteers employed by the ministry who collect or create personal information have taken the CIRMO-developed training course prior to that person providing services for the ministry
- Ensure the ministry is aware of all Service Providers and volunteers that have access to personal information as part of the services they are providing and that a process is in place for communicating notice of changes regarding access to personal information

Privacy Breaches and Information Incidents:

- Act as a liaison and point of contact for issues within the ministry that may arise during an investigation into a Privacy Breach
- Provide the CIRMO, as required, with timelines and follow-up reports on steps taken to ensure implementation of and compliance with recommendations made after a Privacy Breach investigation
- Perform the duties of the MPO as outlined in the Information Incident Management Policy

Compliance Reviews and Audits:

- Conduct their ministry's self-audit and communicate results to the CIRMO as per the Privacy Compliance Audit Policy
- Assist the CIRMO with any compliance review of their ministry's privacy management practices, where necessary
- Ensure necessary information is recorded and retained in support of any future compliance review or audit.

Employees have the responsibility to:

Accountability for Privacy Management:

- Comply with the PMAP and other privacy-related policies, guidelines and templates developed by the CIRMO
- Engage with the CIRMO before contacting the Office of the Information and Privacy Commissioner on matters related to privacy
- Participate in their ministry's efforts to create and maintain an enhanced culture of privacy and the responsible collection, use, disclosure, storage and destruction of personal information

Education & Awareness:

- Complete the training relevant to their job as prescribed by the CIRMO

PIAs, Agreements, Inventories and the PID:

- Conduct Privacy Impact Assessments (PIAs) in the manner and form directed by the CIRMO
- Prepare any agreements (i.e. ISAs, IPAs, RAs) in the manner and form directed by the CIRMO
- Support the CIRMO and MPO in ensuring that the PID and any personal information inventories are accurate and complete

Privacy Breaches and Information Incidents:

- Immediately report actual or suspected Privacy Breaches, including privacy complaints as per the Information Incident Management Policy
- Follow all instructions and recommendations issued by a CIRMO Incident Lead during an information incident investigation

Service Provider Management:

- Include the standard 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 the CIRMO
- Inform MPOs of all Service Providers and volunteers that have access to personal information within the ministry's custody and control

Appendix A – Websites

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

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

Ministry Privacy Officer List:
http://www2.gov.bc.ca/gov/content?id=A749F080FC794D82A2CBD96BABA2ABEC

Ministry Chief Information Officer List:
http://www.cio.gov.bc.ca/cio/about/governance/role_cio/mcio_contact_list.page

PIA Directions, Template and Guidelines:
http://www2.gov.bc.ca/gov/content?id=865A6A7E438E4F148BEA8821DD589605

ISA Guideline:
http://www2.gov.bc.ca/assets/download/AE4EE59333D04CF8866F1F5BE7964C49

ISA Template:
http://www2.gov.bc.ca/assets/download/1585604C70724F56B9BAA7606FB61ECC

Information Incident Management Policy:
http://www2.gov.bc.ca/assets/download/0F9CD1D548D3421AAF8CD67FC8344C29

FOIPPA Delegation Instrument:
http://www2.gov.bc.ca/assets/download/8705C389E0EE44D4AACA7088A1A28229

Sample Research Agreement Form:
http://www2.gov.bc.ca/assets/download/CDB1A0B60DA547838DF0742A4EF95CA0

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

Privacy Protection Schedule:
http://www2.gov.bc.ca/gov/content?id=7D880E86AFC74E148A68A1CD2C0EFA03

PMAP Delegation Instrument: *under development*

PID Policy: *under development*

Privacy Compliance Audit Policy: *under development*

Personal Information Inventory Policy: *under development*