Information Sharing Agreement Guidance

Corporate Information and Records Management Office

BRITISH COLUMBIA

January 2020 | Version 1

TABLE OF CONTENTS

INTRODUCTION

This document provides guidance on the topic of Information Sharing Agreements[1] (ISAs) to support the Information Sharing Agreement Directions (ISA Directions) issued by the minister responsible for the *Freedom of Information and Protection of Privacy Act* (FOIPPA). This ISA guidance seeks to supports the ISA Directions with plain language guidance and addresses questions that ministry employees may have about how to start drafting an ISA, key considerations, and the conversations they should have with their information sharing partner(s). The ISA Sample Template is another tool that will enable ministry employees to easily meet the requirements of the ISA Directions.

AUDIENCE

The ISA Guidance and Sample Template are intended to support ministry employees who are sharing personal information and may want or need to create an ISA to govern the information sharing. Specifically, these tools will help ministry employees interpret, understand and put into practice the ISA Directions. Employees may also wish to look to the Privacy Management and Accountability Policy (PMAP), which outlines further information about roles and responsibilities regarding agreements, such as ISAs and how to ensure they are to be entered into the Personal Information Directory (as required by FOIPPA).

WHAT IS AN INFORMATION SHARING AGREEMENT?

An ISA is an agreement between a public body and another public body, person or group of persons[2], prescribed entity or organization that sets the conditions on the collection, use or disclosure of personal information by the parties to the agreement. These conditions support compliance with the provisions of FOIPPA, other applicable legislation and relevant policy requirements.

PURPOSE OF AN ISA

An ISA is an important tool for:

- documenting information sharing conditions;
- demonstrating compliance with FOIPPA and other legislation when required;
- outlining each party's responsibilities respecting the handling and security of personal information;
- building a trusted information sharing relationship; and
- harmonizing expectations for public bodies subject to different policies or legislation.

An ISA does not provide the authority to share personal information. Rather, it documents the conditions for information sharing that is otherwise authorized by FOIPPA and other applicable law. If a ministry is unsure as to whether the personal information it seeks to exchange is subject to FOIPPA, see section 3 of FOIPPA for more information. Ensure that you consider other statutory obligations that may reference "information sharing" or "personal information". This document provides guidance on the ISA Directions and ISAs in general as they relate to FOIPPA.

An ISA is only used for exchanges (including one-way disclosures) of personal information. Some organizations may choose to document the conditions and responsibilities surrounding the exchange of confidential, non-personal

[1] "Information-sharing Agreements" in the ISA Directions are referred to as "Information Sharing Agreements" in this document.

[2] Under the Interpretation Act, "person" includes a corporation, partnership or party, and the personal or other legal representatives of a person to whom the context can apply according to law.

information, these agreements are not considered ISAs under FOIPPA and best practice is not to use this label to avoid confusion[3].

You should confirm your ministry's statutory obligations regarding ISAs, as your ministry might have its own legislation/regulation pertaining to when an ISA is required or its own legislation/regulation that explicitly authorizes regular information sharing with another public body[4].

Similar to Privacy Impact Assessments (PIAs), ISAs help to demonstrate compliance with FOIPPA or other applicable law and support public bodies in ensuring they are adequately protecting personal information in their custody or under their control. PIAs should be completed for the activities covered by an ISA, rather than each individual ISA.

CONTRACTUAL ENFORCEABILITY

An ISA may take on contractual enforceability or be contained within another legal document, such as the General Services Agreement. However, an ISA is not typically considered a legal contract and does not naturally contain enforceability mechanisms. For further guidance on contractual enforceability, it is recommended that the ministry consult Legal Services Branch (LSB).

DETERMINING WHEN AN ISA IS REQUIRED

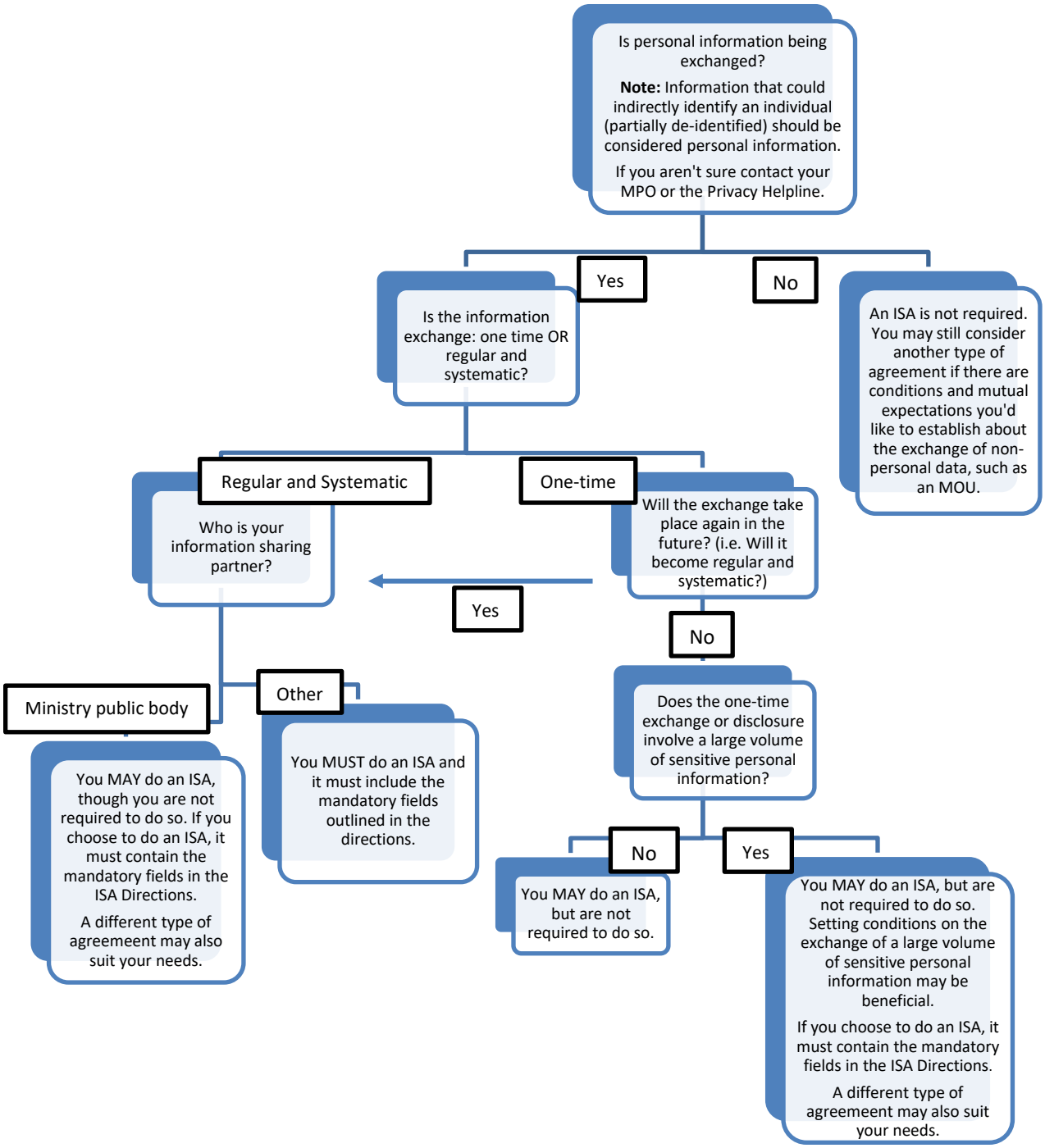
There are times when ISAs are required, and others where ministries can elect to use one. The ISA Directions rely on two considerations to inform whether an ISA is required or optional (and the criteria by which a ministry would choose to use one):

1) The nature of the personal information exchange.
2) The information sharing partner with whom the ministry is sharing personal information.

The below diagram is meant to assist ministries in determining when an ISA is mandatory and when it is discretionary according to the ISA Directions.

[3] Should further guidance on agreements regarding the exchange of non-personal information be developed in the future, the ISA Guidance will be updated to link to relevant resources.

[4] For example, Section 30 of the Employment Assistance Act, which outlines the circumstances in which the minister responsible for that Act may enter into an ISA with certain entities and the circumstances in which prior approval is and is not required by the Lieutenant Governor in Council for these ISAs



MANDATORY ISAS

Ministries must complete an ISA in accordance with the ISA Directions, unless granted an exemption by the Corporate Information and Records Management Office (CIRMO), as described in PMAP. For example, an exemption may be granted where one party has the authority to oblige production of personal information.

Ministries MUST enter into an ISA if all three of the following conditions are met:

- information shared is personal information,

- information sharing is regular and systematic, and
- information sharing partner is not a BC ministry

Below is a list of the categories of partners with whom an ISA is required when sharing personal information, and key considerations for ISAs with each of these partners.

PERSONAL INFORMATION EXCHANGES WITH NON-MINISTRY PUBLIC BODIES SUBJECT TO FOIPPA

E.g. Local public bodies (e.g. universities, health authorities) or FOIPPA Schedule 2 public bodies (such as the Blueberry Industry Development Council, British Columbia Lottery Corporation, etc.)

- Direction B(3) of the ISA Directions contains a list of required information to include in the ISA.
- If legislation or policy applies to all parties, the agreement does not need to restate provisions contained within them. However, the agreement may benefit from referencing the common obligations from the legislation (e.g. "All parties acknowledge they are subject to FOIPPA.").
- Direction B(4) of the ISA Directions contains a list of discretionary information that may be included in an ISA. For example, the ministry may wish to document what they consider to be "reasonable security measures" or who will report an information incident to the BC government's Information Incident Investigations Unit.

PERSONAL INFORMATION EXCHANGES WITH PUBLIC ENTITIES THAT ARE NOT SUBJECT TO FOIPPA

E.g. Other jurisdictions including municipalities outside of BC, other provinces or territories or the federal government.

- Direction B(3) of the ISA Directions contains a list of required information to include in the ISA.
- Direction B(4) of the ISA Directions contains a list of discretionary information that may be included in an ISA.
- When entering into an ISA with a public entity that is not covered by BC's FOIPPA, the ministry should consider whether they intend to negotiate comparable privacy protections and other obligations contained within FOIPPA.

PERSONAL INFORMATION EXCHANGES WITH PRIVATE SECTOR ORGANIZATIONS

The ministry should carefully consider what the appropriate relationship is between the Province and the private sector organization. The ministry should consider whether it is an information sharing relationship (i.e. partners), or rather, it is a service provider relationship (i.e. one body is contracted to the other).

- If it is an information sharing relationship, then the ISA is the appropriate mechanism to document mutually agreed upon conditions. The ministry must engage their Ministry Privacy Officer (MPO) before entering an ISA when it is outside of a service provider relationship. If you have questions about this, you may contact the Privacy and Access Helpline[5]. The ministry may wish to engage LSB for support. If this type of arrangement happens frequently in your ministry, facilitating this engagement once may be enough to figure out your long-term strategy for future arrangements.
- If it is a service provider relationship, an ISA is unlikely to be the most appropriate tool and documentation should be in contract. The Privacy Protection Schedule (PPS), which must be included in all contracts between a service provider (e.g. a non-profit organization or private company) and a ministry is likely the most appropriate mechanism to ensure compliance. The PPS ensures that the ministry has communicated its obligations under FOIPPA to the service provider and contains the appropriate enforcement mechanisms. The ministry must

[5] The Privacy and Access Helpline can be reached at privacy.helpline@gov.bc.ca or (250) 356-1851/toll-free 1-800-663-7867.

engage the Privacy and Access Helpline if they intend to include additional information sharing provisions beyond the standard terms of the PPS.

- Any additional information sharing conditions the ministry wishes to set on the personal information exchange, beyond those included in the PPS can be included in the service provider's contract dependent on consultation with legal counsel and the Privacy, Compliance and Training Branch (PCT).

FACTORS ASSOCIATED WITH THE INFORMATION SHARING EXCHANGE

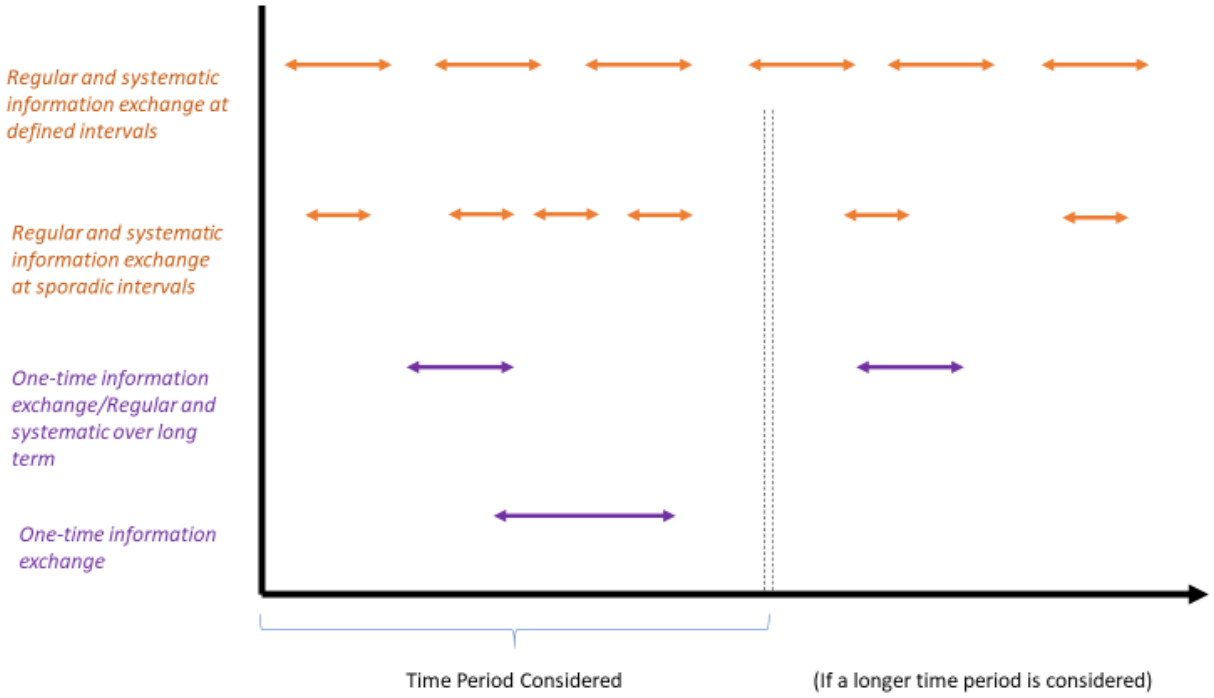
'Information sharing exchange' refers to a collection or disclosure and can be a one-way exchange (from one partner to one or more other partners) or a reciprocal exchange (the information flows both ways between partners). The exchange can be regular and systematic, or one-time. If information sharing is regular and systematic you may be required to enter into an ISA.

> Regular means the personal information is shared on a habitual, usual, customary, patterned, normal, routine, frequent, or typical basis (e.g. monthly confirmation that a professional is in good standing with their regulating body which happens on a defined schedule), though not necessarily on a known interval. This definition does not include information exchanges that happen one time or those that are random or inconsistent (e.g. on-demand or unpredictable).
>
> Systematic means the personal information is shared using a plan or system that can be fixed, methodical, standardized, or repeated (e.g. reporting using the same mechanism for exchange on an ongoing program or activity).

- Example 1: There may be regular and systematic personal information exchanges between the crown corporations who can access an eLearning system and the Public Service Agency, which hosts it.
- Example 2: A branch that collects payment information through an application managed by the Ministry of Finance (FIN) may collect and disclose personal identity and financial information "systematically," through various payment apps and disclosures of this information may also be on a regular basis (i.e., every Friday, every night at midnight, etc.).
- Example 3: A ministry may make disclosures about a specific individual to a professional occupations' regulating body. Considered in isolation, those disclosures might be considered as one-time. But if you view all the disclosures of this nature the ministry makes over time, the ministry may assess them as regular.

In all three of the above examples, an ISA would be required.

Pay close attention to when an information exchange appears to be one-time. In some cases, an ISA might be required because, when considered over time, the exchange could ultimately be regular. This could mean that an ISA that at first appears to be discretionary is in fact mandatory. If you initially think the information sharing will only occur once, regular follow-up requests from the same source could indicate the need to enter into an ISA. For support in making this determination consult your MPO.



If you are unsure whether your information sharing requires an ISA, you may wish to consider the following questions:

- Do you anticipate there could be future information exchanges? Have you asked your information sharing partner about potential future exchanges to determine whether your information exchange could be considered regular and systematic?
- Is the content valuable and likely to change? Will updates be sought or required in the future by an information sharing partner?

If you are still unsure or have any questions, please contact your MPO or the Privacy and Access Helpline .

DE-IDENTIFIED INFORMATION

You may be required to do an ISA if you are considering the exchange of personal information that has been partially-de-identified (where some personal information has been removed but may still be identifiable). For example, if partially de-identified personal information is being exchanged with a ministry public body, you may do an ISA, though you are not required to do so.

Consult your MPO and/or the Privacy and Access Helpline for support regarding the de-identification of personal information.

DISCRETIONARY ISAS

The ISA Directions recognize that ministries may opt to enter into ISAs where they are not required under the ISA Directions (e.g. ministry to ministry information exchanges). Whether or not a ministry chooses to do so will be dependent on who the ministry is exchanging information with, the regulatory requirements of that ministry (i.e. another enactment requiring ISAs) and what kind of personal information is being exchanged. Ministries have the

option to enter into a discretionary ISA where, for example, an ISA would contribute to the protection of particularly sensitive personal information or minimize risk in unique information sharing circumstances.

If a ministry enters into a discretionary ISA, the ISA must still meet the minimum requirements set out in the ISA Directions (i.e. the ISA MUST include all of the mandatory fields).

PERSONAL INFORMATION EXCHANGES BETWEEN MINISTRIES

Ministries may enter into an ISA where the exchange is within one ministry (intra-ministry) or between two ministries (inter-ministry). Ministries may want to consider this where one or more of the parties wish to set additional conditions on the information sharing beyond those found in applicable legislation and policy.

ISAs between ministries are not mandatory under the ISA Directions (although they could be required under another enactment), as each party to the agreement are bound by the same general legal and policy obligations. In light of these considerations it may be worth considering if an ISA would add value, given the additional time required to prepare an agreement which may not be necessary.

The ISA need not restate commonly shared obligations between parties (e.g. obligations stemming from FOIPPA, PMAP, Information Incident Management Policy, Information Management Practice Reviews, Information Security Policy etc.). Restating shared obligations may not be useful, but rather stating how the partners will meet the shared obligation may be (e.g. you need not state that information incidents need to be reported but may wish to be clear who will report information incidents, as required).

FACTORS ASSOCIATED WITH THE INFORMATION SHARING EXCHANGE

Ministries may enter into an ISA if the information sharing exchange is a one-time collection or disclosure. To determine whether or not this would be advisable, consider the guidance above regarding disclosures of sensitive personal information and whether an ISA would add value to the exchange. Your ministry may also have guidance or requirements for documenting one-time only collections/disclosures of personal information. If you need support in making this determination, contact your MPO or the Privacy and Access Helpline.

DRAFTING AN INFORMATION SHARING AGREEMENT

START WITH A CONVERSATION

An ISA will have the most value if each party considers the information, the exchange, and the conditions that are important. For this reason, the first step in creating an ISA is to have a conversation with your information sharing partners. Having these discussions up front will help facilitate the drafting process. We recommend you consider the following questions in your initial discussion. Additionally, if a ministry wants to enter into an ISA with another ministry, consider what the ISA would accomplish that is not already covered under the shared requirements of FOIPPA. This is not an exhaustive list of the mandatory considerations, but rather a list of the high level-questions to support initiating the ISA drafting process:

1. What is the purpose for the information sharing?
2. What information is going to be shared?
3. Is the information sharing ongoing, frequent or one time?
4. What is the intended use for this data and is it authorized by FOIPPA?
5. Who within the public body or organization will have access to the information?

6. Are the parties subject to any of the same laws or policies? What information do those parties control?
7. What special conditions or considerations should be reflected in your information sharing agreement? Are there particular conditions or protections you would like to ensure all partners have in place?
8. What are the partners' mutual expectations about notification and responses to an information incident/breach?
9. How will you ensure the personal information you are exchanging is accurate and up-to-date?
10. Are there limitations on further use of the shared information?
11. What safeguards are in place to prevent unauthorized collection, use and disclosure of the shared information?
12. How will you dispose of information that has been shared and is no longer needed (i.e. do you both have the same retention schedules)?

USING THE INFORMATION-SHARING AGREEMENT SAMPLE TEMPLATE

The ISA Directions provide a list of information the ministry must include (mandatory) as well as information the ministry can choose to include (discretionary). The ISA Sample Template provided by CIRMO will include language that addresses each of these provisions. Should a ministry develop their own template, it must include all items included in Direction B(3) of the ISA Directions. However, ministries are not required to use the language provided in the sample template nor the sample template itself. Rather, ministries are encouraged to do so (when the sample template is released) because the language will have been reviewed by LSB and PCT.

DRAFTING CONSIDERATIONS

FORMAT

The format for an ISA is intentionally flexible and may be represented in many types of documentation, including but not limited to a Memorandum of Understanding, Memorandum of Agreement, Terms of Use or a Common or Integrated Program Agreement. This allows the ministry to determine the most logical and appropriate form of documentation.

Ministry employees must ensure that the ISA, regardless of document type, is reported to their MPO. The MPO must ensure that all ISAs (regardless of document type) are recorded in the Personal Information Directory (PID) by reporting ISAs outside of the PIA process to the Privacy and Access Helpline. The PID is a public directory that provides short summaries of government's ISAs, among other holdings.

LEVEL OF DETAIL

The ISA Directions require that a "reasonable level of detail" be included for the mandatory categories of conditions. For example, it is not necessary to list the individual elements of personal information being shared, rather a high-level description of the type(s) of personal information will suffice.

The information sharing partners require enough information to understand the intention of the information exchange, the ISA and the conditions within it. Remember this is not usually a legal contract; using plain language will normally make the ISA more useful. The ISA Sample Template contains generic provisions that are available to you, can be used verbatim (as appropriate), or as a guide in drafting subject-specific conditions.

Some ministries have a unique approach to ISAs. Some ministries have legislated requirements distinct from FOIPPA or have ministry-specific policy or process. If you are tasked with the development of an ISA, begin by engaging your

MPO. The process for developing ISAs may vary between ministries and your MPO will be able to advise on how to proceed in your ministry.

RECORDS OBLIGATIONS

When an ISA is developed for use by a ministry and a public body[6] that is subject to the *Information Management Act* (IMA), you may identify the relevant information schedules (i.e. ARCS and ORCS) in the ISA, and, if so, any possible discrepancies in retention requirements should be addressed. If any of the records subject to the agreement are not covered by an approved information schedule, appropriate retention arrangements should be agreed upon and documented in the ISA itself with the understanding that these will need to be revisited when information schedules are developed.

When an ISA is developed between a government body covered by the IMA and a public body not covered by the IMA, the ISA should document the records retention requirements for both parties and reflect the relevant information schedule and/or appropriate retention requirements. It is not necessary for both parties to an ISA to retain the information for the same amount of time. If one of the public bodies is not subject to the IMA, it may be appropriate for its copy of the information to be destroyed as soon as it is no longer required, in accordance with the ISA.

The ministry should consult its Government Records Service contact about the recordkeeping requirements documented in the ISA.

TERM

Per the ISA Directions, the ministry is required to note the date the ISA is effective, and, if it is applicable, the date on which the ISA will cease to have effect.

It is recommended that the ISA assign a term for the exchange of personal information including the start and end date. Term length should be determined based on the volume, sensitivity and/or regularity with which the information is exchanged. Further, the information sharing partners should consider whether the conditions within the ISA are likely to require amendment. This is likely influenced by the volume and specificity of conditions.

LEGAL REVIEW

It is a common perception in government that a legal review must be conducted by LSB before an ISA can enter the approval process. Ultimately this is a ministry decision, but there is no corporate policy or legal requirement that an ISA be reviewed by LSB. The ministry should consider whether there is value in additional legal review, particularly if the ministry intends to use the language provided in the sample template. LSB should be consulted if the ministry intends to include ISA provisions within a contractually enforceable document.

APPROVAL PROCESS

The determination of who should appropriately complete and approve an ISA (i.e. the signatory) should be made based on the type, volume, sensitivity and overall risk associated with the personal information exchanged. Ministries should consider who in the Ministry should be responsible for the renewal, amendment and ultimately

[6] Reference to public bodies in this section refers to public bodies subject to FOIPPA that are also government bodies under the IMA. For more information see the IMA Regulation. For information on public bodies subject to FOIPPA, see FOIPPA Schedule 1

the approval of the ISA on behalf of the head, unless your ministry has legislation that specifically outlines these responsibilities. This guidance should not be interpreted to override formal delegation instruments and/or Orders in Council contained within ministry-specific legislation (e.g. the Child, Family and Community Service Act).

APPENDIX A – GLOSSARY

Administrative Records Classification System (ARCS) means the government-wide standard for classifying, filing, retrieving and disposing of administrative and other common records. These records support functions such as the management of facilities, finance, personnel, and information systems.

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 in relation to a public body, includes a volunteer, and a service provider.

Information Incident Management Policy means the policy that provides direction to guide employees and business owners (including supervisors and contract service providers) in responding to incidents that threaten information privacy or security).

Information Management Practice Reviews assess the maturity of information management practices in ministries.

Information Security Policy means the policy that acts as the framework under which all ministries must operate in order to ensure the information security practices of the Government of BC are reasonable, appropriate, and efficient. It provides the foundation for the information security governance program, which includes standards, procedures, training and awareness material, all of which are used to protect government information and information systems.

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 Electronic 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 a group of persons;
(f) a prescribed entity,

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

Information Sharing Agreement Directions outline the requirements related to Information Sharing Agreements, including the mandatory and discretionary types of information for ministries to include when preparing information sharing agreements.

Memorandum of Agreement or Memorandum of Understanding generally refers to a document that describes the general principles of an agreement between parties, but does not amount to a substantive contract.

Ministry Privacy Officer means the designated individual from each ministry accountable for privacy within their ministry.

Operational Records Classification Systems (ORCS) means the integrated records classification and scheduling system tailored for a specific function or program of government in accordance with the Information Management Act and other relevant legislation. Like ARCS, ORCS facilitate classification, filing, retrieval and disposition.

Partial De-Identification means a de-identification process that removes direct identifiers and may manage the indirect identifiers that could potentially be combined to identify an individual. Partially de-identified records contain personal information; therefore, the disclosure of partially de-identified records would require appropriate authorization under Part 3 of FOIPPA. Some partially de-identified information may also be referred to as pseudonymized data.

Person means a corporation, partnership or party, and the personal or other legal representatives of a person to whom the context can apply according to law. In the context of some section, "person" will clearly mean an individual; i.e., a human being.

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

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.

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.

Privacy Management and Accountability Policy is the policy 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 supports compliance with the privacy requirements of the Freedom of Information and Protection of Privacy Act (FOIPPA).

Organization includes a person, an unincorporated association, a trade union, a trust or a not for profit organization, but does not include

(a) an individual acting in a personal or domestic capacity or acting as an employee,
(b) a public body,
(c) the Provincial Court, the Supreme Court or the Court of Appeal,
(d) the Nisga'a Government, as defined in the Nisga'a Final Agreement, or
(e) a private trust for the benefit of one or more designated individuals who are friends or members of the family of the settlor;

Public body means

(a) a ministry of the government of British Columbia,

(b) an agency, board, commission, corporation, office or other body designated in, or added by regulation to, Schedule 2, or
(c) a local public body

but does not include

(d) the office of a person who is a member or officer of the Legislative Assembly, or
(e) the Court of Appeal, Supreme Court or Provincial Court.

Regular means the personal information is shared on a habitual, usual, customary, patterned, normal, routine, frequent, or typical basis (e.g. monthly confirmation that a professional is in good standing with their regulating body which happens on a defined schedule), though not necessarily on a known interval. This definition does not include information exchanges that happen one time or those that are random or inconsistent (e.g. on-demand or unpredictable).

Service Provider means a person retained under a contract to perform services for a public body.

Systematic means the personal information is shared using a plan or system than can be fixed, methodical, standardized, or repeated.

Terms of Use means the rules by which one must agree to abide in order to use a service.