Annex A

Canadian Domestic Laws Applicable to the Certification Activities of an Accountability Agent under the APEC Cross Border Privacy Rules System

An APEC-recognized Accountability Agent is responsible for assessing, certifying, monitoring and enforcing company compliance with the CBPR Program requirements.

To become an APEC- recognized Accountability Agent, an applicant must complete and sign the Accountability Agent APEC Recognition Application. By signing, submitting and publicly releasing the Recognition Application, an applicant represents that the answers contained in the Recognition Application are true.

An Accountability Agent that publicly communicates its participation in the CBPR System is making a representation that it complies with all the requirements applicable to an APEC-recognized Accountability Agent, including those related to the review, certification, monitoring of companies' compliance with the CBPR program requirements.

By publicly displaying a list of companies that it has certified as compliant with the CBPR Program requirements, the Accountability Agent is making representations about the compliance of these companies with the CBPR program requirements.

APEC-recognized CBPR Accountability Agents operating in Canada may be subject to the following domestic laws in respect of their certification activities, as follows:

COMPETITION ACT

Part Vll of Canada's *Competition Act*, addresses false or misleading representations and deceptive marketing practices when promoting the supply or use of a product or any business interest. All representations, in any form whatever, that are false or misleading in a material respect are subject to the Act. If a representation could influence a consumer to buy or use the product or service advertised, it is material. To determine whether a representation is false or misleading, the courts consider the "general impression" it conveys, as well as its literal meaning.

Canada's Competition Bureau conducts investigations in respect of contraventions of the Competition Act. The Act provides two adjudicative regimes to address false or misleading representations and deceptive marketing practices.

Under the criminal regime, the general provision prohibits all materially false or misleading representations made knowingly or recklessly. Under the civil regime, the general provision prohibits all materially false or misleading representations. Other provisions specifically prohibit performance representations that are not based on adequate and proper tests, misleading warranties and guarantees, untrue, misleading or unauthorized use of tests and testimonials, etc.

Under the criminal regime, certain practices are brought before the criminal courts, requiring proof of each element of the offence beyond a reasonable doubt. On summary conviction, the person is liable to a fine and/or imprisonment. If convicted on indictment, the person is liable to a fine at the discretion of the

court and/or imprisonment. Under the civil regime, certain practices may be brought before the Competition Tribunal, the Federal Court or the superior court of a province and require that each element of the conduct be proven on a balance of probabilities. The court may order a person to cease the activity, publish a notice, pay an administrative monetary penalty or it may also issue an order for restitution to be paid.

TRADE-MARKS ACT

Trademarks may be one or a combination of words, sounds or designs used to distinguish the goods or services of one person or organization from those of others in the marketplace. A trademark includes, but is not limited to certification marks, which are registered by an individual or organization, and licensed to others for the purpose of identifying goods or services that meet a defined standard.

More precisely, section 2 of the *Trade-marks Act* defines a certification mark as a mark that is used for the purpose of distinguishing wares or services that are of a defined standard with respect to:

1. the character or quality of the wares or services;
2. the conditions under which the wares have been produced or the services performed;
3. the class of persons by whom the wares have been produced or the services performed; or
4. the area within which the wares have been produced or the services performed.

Section 7 of the Act prohibits the use of any description, in association with a ware or service, that is false in a material sense and is likely to mislead the public, including (but not limited to) those related to the character, quality, or the performance of a ware or service.

Section 23(1) of the Trade-marks Act specifies that a certification mark may be adopted and registered only by a person who is not engaged in the manufacture, sale, leasing or hiring of wares or the performance of services such as those in association with which the certification mark is used. Pursuant to s. 57 of the Act, the Federal Court of Canada could cancel a mark if an owner engages in these activities.

Section 23 (2) of the Act allows the owner of a certification mark to license others to use the mark in association with wares or services that meet the defined standard defined by the owner.

Under s. 23(3), the owner of a registered certification mark may prevent its use by unlicensed persons or in association with any wares or services in respect of which the mark is registered but to which the licence does not extend. In other words, the owner may prevent the use of the mark by those to whom the owner has not licensed the mark or who use it inaccurately or incorrectly, including by applying the mark to services that do not meet the owner's defined standard.

Licensees may also commence legal proceedings under the Trade-marks Act. Under s. 50(3), the licensee is permitted to call on the owner to undertake proceedings for infringement, and, if the owner refuses or neglects to do so within two months, the licensee may institute proceedings for infringement in their own name, making the owner a defendant.

With the combined effect of s. 45 of the Act and either s. 50 or s. 23(2) of the Act, lack of control by the owner could also lead to the cancellation of the mark by the Canadian Intellectual Property Office (CIPO).

ANNEX B

APEC CROSS-BORDER PRIVACY RULES SYSTEM PROGRAM REQUIREMENTS: ENFORCEMENT MAP

The purpose of this Annex is to describe Canada's ability to take enforcement action under Part 1 of the *Personal information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5 , having the effect of protecting personal information consistently with the CBPR Program Requirements. Further, Column 3 of the following table identifies provisions in Part 1 of Canada's PIPEDA which set requirements that have the effect of establishing a level of protection for personal information that is consistent with each of the CBPR System Program Requirements.

PIPEDA establishes rules governing the collection, use and disclosure of personal information by organizations in the course of a commercial activity. The Act applies to all organizations in every sector of the economy.

Pursuant to paragraph 26(2)(b) of the Act, organizations or activities subject to provincial laws that have been deemed substantially similar by Governor in Council, have, by Order, been exempt from PIPEDA in respect of the collection, use or disclosure of personal information within these provinces. PIPEDA continues to apply to the collection, use or disclosure of personal information in connection with the operations of a federal work, undertaking or business in all provinces and territories, as well as to the collection use or disclosure of personal information outside provinces, territories or country. PIPEDA also applies to all federal works, undertakings and businesses in respect of employee personal information.

Enforcement for PIPEDA relies on an ombudsman model, with oversight and redress mechanisms provided through the Privacy Commissioner of Canada and the Federal Court. Section 12 of the Act empowers the Commissioner to receive and investigate complaints respecting an organization's compliance with any of the requirements contained in PIPEDA. He may, pursuant to s. 12(2) of the Act, resolve privacy conflicts through various dispute resolution mechanisms. At the conclusion of an investigation, the Commissioner is required to release a report outlining the Commissioner's findings and recommendations, including any settlement reached and notice of action taken (s.13). Complainants, including the Commissioner may also apply to the Federal Court for a hearing in respect of any matter pertaining to a complaint (s. 14 and s. 15). The court is empowered to order organizations to change their practices and can also award damages to the aggrieved (s. 16).

Note: The information provided in this Annex is not intended to represent all obligations provided under PIPEDA, nor does it purport to provide a complete and comprehensive account of the Privacy Commissioner of Canada's powers under that Act. This information is not intended to be relied on as legal advice and should not be used as interpretation of legal obligations contained in PIPEDA.

ENFORCEMENT MAP

NOTICE

Assessment Purpose – *To ensure that individuals understand the applicant's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.*

NOTICE

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy*)**
1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.	If **YES,** the Accountability Agent must verify that the Applicant's privacy practices and policy (or other privacy statement) include the following characteristics: • Available on the Applicant's Website, such as text on a Web page, link from URL, attached document, pop-up windows, included on frequently asked questions (FAQs), or other (must be specified). • Is in accordance with the principles of the APEC Privacy Framework; • Is easy to find and accessible; • Applies to all personal information; whether collected online or offline; • States an effective date of Privacy	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. **Clause 4.8** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. **Clause 4.8.1** Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be

	Statement publication. Where Applicant answers **NO** to question 1, and does not identify an applicable qualification subject to the Qualifications to Notice set out below, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	made available in a form that is generally understandable. **Clause 4.8.2** The information made available shall include (*a*) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded; (*b*) the means of gaining access to personal information held by the organization; (*c*) a description of the type of personal information held by the organization, including a general account of its use; (*d*) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and (*e*) what personal information is made available to related organizations (e.g., subsidiaries). **Clause 4.8.3** An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.
1.a) Does this privacy statement describe how personal information is collected?	If **YES**, the Accountability Agent must verify that: • The statement describes the collection practices and policies applied to all covered personal information collected by the Applicant.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

	• The Privacy Statement indicates what types of personal information, whether collected directly or through a third party or agent, is collected, and • The Privacy Statement reports the categories or specific sources of all categories of personal information collected. If **NO**, the Accountability Agent must inform the Applicant that Notice as described herein is required for compliance with this principle.	**Clause 4.2.3** The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. **Clause 4.2.5** Persons collecting personal information should be ab le to explain to individuals the purposes for which the information is being collected. **Clause 4.4.1**: Organizations shall specify the type of information collected as part of their information-handling policies and practices in accordance with the Openness principle **Clause 4.8** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. **Clause 4.8.1** Organizations shall be open about their policies and practices with respect to the management of personal information. … **Clause 4.8.2** The information made available shall include … (*b*) the means of gaining access to personal information held by the organization; … (*e*) what personal information is made available to related organizations (e.g., subsidiaries).

1.b) Does this privacy statement describe the purpose(s) for which personal information is collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the applicant provides notice to individuals of the purpose for which personal information is being collected. Where the Applicant answers **NO** and does not identify an applicable qualification set out below, the Accountability Agent must notify the Applicant that notice of the purposes for which personal information is collected is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	***Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. **Clause 4.2.1** The organization shall document the purposes for which personal information is collected in order to comply with the Openness Principle (clause 4.8) and the Individual Access Principle (clause 4.9) **Clause 4.2.3** The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. **Clause 4.2.5** Persons collecting personal information should be ab le to explain to individuals the purposes for which the information is being collected.
1.c) Does this privacy statement inform individuals whether their personal information is made available to third parties and for what purpose?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and the purpose for which the personal information will or may be made available. Where the Applicant answers **NO** and does not identify an applicable	***Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.8** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. **Clause 4.8.1** Organizations shall be open about their policies and practices with respect to the

	qualification, the Accountability Agent must notify the Applicant that notice that personal information will be available to third parties is required and must be included in their Privacy Statement. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	management of personal information. … **Clause 4.8.2** The information made available shall include … (*e*) what personal information is made available to related organizations (e.g., subsidiaries). **Clause 4.3.1** … The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.
1.d) Does this privacy statement disclose the name of the applicant's company and location, including contact information regarding practices and handling of personal information upon collection? Where YES describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides name, address and a functional e-mail address. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that such disclosure of information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles. **Clause 4.8.2** The information made available shall include (*a*) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded; (*b*) the means of gaining access to personal information held by the organization; (*c*) a description of the type of personal information held by the organization, including a general account of its use; (*d*) a copy of any brochures or other information that explain the organization's policies, standards, or codes; …

1.e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's Privacy Statement includes, if applicable, information regarding the use and disclosure of all personal information collected. Refer to question 8 for guidance on permissible uses of personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant, that such information is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	***Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.3.1** … The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. **Clause 4.8** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information. **Clause 4.8.1** Organizations shall be open about their policies and practices with respect to the management of personal information. … **Clause 4.8.2** The information made available shall include … (*c*) a description of the type of personal information held by the organization, including a general account of its use… and (*e*) what personal information is made available to related organizations (e.g., subsidiaries).
1.f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Privacy Statement includes: • The process through which the individual may access his or her personal information (including electronic or traditional non- electronic means).	***Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.8** An organization shall make readily available to individuals specific information about its policies and practices relating to the management of

	• The process that an individual must follow in order to correct his or her personal information. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that providing information about access and correction, including the Applicant's typical response times for access and correction requests, is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	personal information. **Clause 4.8.1** Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable. **Clause 4.8.2** The information made available shall include (*b*) the means of gaining access to personal information held by the organization; (*c*) a description of the type of personal information held by the organization, including a general account of its use; (*d*) a copy of any brochures or other information that explain the organization's policies, standards, or codes; …
2. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you provide notice that such information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information is being (or, if not practicable, has been) collected and that the notice is reasonably available to individuals. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the notice that personal information is being collected is required for compliance with	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. **Clause 4.2.3** The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is

	this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	collected. **Clause 4.2.5** Persons collecting personal information should be ab le to explain to individuals the purposes for which the information is being collected.
3. Subject to the qualifications listed below, at the time of collection of personal information (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant explains to individuals the purposes for which personal information is being collected. The purposes must be communicated orally or in writing, for example on the Applicant's website, such as text on a website link from URL, attached documents, pop-up window, or other. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant of the need to provide notice to individuals of the purposes for which personal information is being collected. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. **Clause 4.2.3** The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. **Clause 4.2.4** When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. … **Clause 4.2.5** Persons collecting personal information should be ab le to explain to individuals the purposes for which the information is being collected. **Clause 4.3.1** … The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.

		Clause 4.5 Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual … **Clause 4.5.1** Organizations using personal information for a new purpose shall document this purpose.
4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides notice to individuals that their personal information will be or may be shared with third parties and for what purposes. Where the Applicant answers **NO** and does not identify an applicable qualification set out on part II of the CBPR Self-Assessment Guidelines for Organisations, the Accountability Agent must inform the Applicant to provide notice to individuals that the personal information collected may be shared with third parties. Where the Applicant identifies an applicable qualification, the Accountability Agent must determine whether the applicable qualification is justified.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2:** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. **Clause 4.2.3** The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. **Clause 4.2.4** When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. … **Clause 4.2.5** Persons collecting personal information should be ab le to explain to individuals the purposes for which the information is being collected. **Clause 4.5** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the

		individual …

COLLECTION LIMITATION

Assessment Purpose - *Ensuring that collection of information is limited to the specific purposes stated at the time of collection. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair.*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy*)**
5. How do you obtain personal information: 5.a) Directly from the individual? 5.b) From third parties collecting on your behalf? 5.c) Other. If YES, describe.	The Accountability Agent must verify that the Applicant indicates from whom they obtain personal information. Where the Applicant answers **YES** to any of these sub- parts, the Accountability Agent must verify the Applicant's practices in this regard. There should be at least one 'yes' answer to these three questions. If not, the Accountability Agent must inform the Applicant that it has incorrectly completed the questionnaire.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.3** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate. **Clause 4.4** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?	Where the Applicant answers **YES** and indicates it only collects personal information which is relevant to the identified collection purpose or other compatible or related purposes, the Accountability Agent must require the Applicant to identify:	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Part 1 – Division 1: Protection of personal information**

	• Each type of data collected; • The corresponding stated purpose of collection for each; and • All uses that apply to each type of data; • An explanation of the compatibility or relatedness of each identified use with the stated purpose of collection. Using the above, the Accountability Agent will verify that the applicant limits the amount and type of personal information to that which is relevant to fulfill the stated purposes. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that it must limit the use of collected personal information to those uses that are relevant to fulfilling the purpose(s) for which it is collected.	**Subsection 5 (3)** An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances. **Schedule 1** **Clause 4.4** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means. **Clause 4.4.1** Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).
7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.	Where the Applicant answers **YES,** the Accountability Agent must require the Applicant to certify that it is aware of and complying with the requirements of the jurisdiction that governs the collection of such personal information and that it is collecting information by fair means, without deception. Where the Applicant Answers **NO**, the Accountability Agent must inform that Applicant that lawful and fair procedures are required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Part 1 – Division 1: Protection of personal information** **Subsection 5 (3)** An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

		Schedule 1 **Clause 4.4** The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means. **Clause 4.4.2** The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

USES OF PERSONAL INFORMATION

Assessment Purpose - *Ensuring that the use of personal information is limited to fulfilling the specific purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant.*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy*)**
8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection, to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of written policies and procedures to ensure that] all covered personal information collected either directly or indirectly through an agent is done so in accordance with the purposes for which the information was collected as identified in the Applicant's Privacy Statement(s) in effect at the time of collection or for other compatible or related purposes. Where the Applicant Answers **NO**, the Accountability Agent must consider answers to Question 9 below.	***Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.5** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes. **Clause 4.2.4:** When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before the information can be used for that purpose.

		Clause 4.3.1 Consent is required for the collection of personal information and the subsequent use or disclosure of this information. … The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.
9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below. 9.a) Based on express consent of the individual? 9.b) Compelled by applicable laws?	Where the Applicant answers **NO** to question 8, the Applicant must clarify under what circumstances it uses personal information for purposes unrelated to the purposes of collection and specify those purposes. Where the applicant selects 9a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained, and the Accountability Agent must verify that the Applicant's use of the personal information is based on express consent of the individual (9.a), such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify)	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.3.1** Consent is required for the collection of personal information and the subsequent use or disclosure of this information. … The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. **Clause 4.5** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. **Part 1 – Division 1: Protection of personal information** 7(2)(d) …an organization may, without the knowledge or consent of the individual, use personal information without the knowledge or consent of the individual only if … (*d*) it was

	Where the Applicant answers 9.a, the Accountability Agent must require the Applicant to provide a description of how such consent was obtained. The consent must meet the requirements set forth in questions 17-19 below. Where the Applicant selects 9.b, the Accountability Agent must require the Applicant to provide a description of how the collected personal information may be shared, used or disclosed as compelled by law. Where the Applicant does not answer 9.a or 9.b, the Accountability Agent must inform the Applicant that limiting the use of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	collected under paragraph 7(1) … (e). 7(1)(e) **…** an organization may collect personal information without the knowledge or consent of the individual only if the collection is made for the purpose of making a disclosure (i) ... , or (ii) that is required by law.
10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.	Where the Applicant answers **YES** in questions 10 and 11, the Accountability Agent must verify that if personal information is disclosed to other personal information controllers or transferred to processors, such disclosure and/or transfer must be undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual, or compelled by law.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.5** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

	Also, the Accountability Agent must require the Applicant to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Using the above, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.	**Clause 4.2.4:** When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before the information can be used for that purpose. **Clause 4.3.1** Consent is required for the collection of personal information and the subsequent use or disclosure of this information. … The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used.
11. Do you transfer personal information to personal information processors? If YES, describe.		***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? If YES, describe.		***Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.5** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes. **Clause 4.2.4:** When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before the information can be used for that purpose.
13. If you answered NO to question 12 or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances? 13.a) Based on express consent of the individual? 13.b) Necessary to provide a service or product requested by the individual? 13.c) Compelled by applicable laws?	Where applicant answers **NO** to question 13, the Applicant must clarify under what circumstances it discloses or transfers personal information for unrelated purposes, specify those purposes. Where the Applicant answers **YES** to 13.a, the Accountability Agent must require the Applicant to provide a description of how individual's provide consent to having their personal information disclosed and/or transferred for an unrelated use, such as: • Online at point of collection • Via e-mail	***Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.5** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

	• Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) Where the Applicant answers **YES** to 13.b, the Accountability Agent must require the Applicant to provide a description of how the disclosure and/or transfer of collected personal information is necessary to provide a service or product requested by the individual. The Accountability Agent must verify that the disclosure or transfer is necessary to provide a service or product requested by the individual. Where the Applicant answers **YES** to 13.c, the Accountability Agent must require the Applicant to provide a description of how collected information may be shared, used or disclosed as compelled by law. The Applicant must also outline the legal requirements under which it is compelled to share the personal information, unless the Applicant is bound by confidentiality requirements. The Accountability Agent must verify the existence and applicability of the legal requirement. Where the Applicant answers **NO** to 13.a, b and c, the Accountability Agent must inform the Applicant that limiting the disclosure and/or transfer of collected information to the identified purposes of collection or other compatible or related purposes, unless permitted under the circumstances listed in this Question, is required for compliance with this principle.	**Clause 4.2.4:** When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before the information can be used for that purpose. **Clause 4.3.1** Consent is required for the collection of personal information and the subsequent use or disclosure of this information. … **Clause 4.3.4** The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. **Clause 4.3.6** The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney). **Part 1 – Division 1: Protection of Personal Information**

		Subsection 7(3)(c) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, disclose personal information without the knowledge or consent of the individual only if the disclosure is required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records; **Subsection 7(3)(i)** For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, disclose personal information without the knowledge or consent of the individual only if the disclosure is <u>required by law</u>;

CHOICE

Assessment Purpose - *Ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in part II of the CBPR Self-Assessment Guidelines for Organisations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy*)**
14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of the mechanisms provided to individuals so that they may exercise choice in relation to the collection of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these mechanisms are in place and operational and that the purpose of collection is clearly stated. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification and the Accountability Agent must verify whether the	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. **Clause 4.2.3:** The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. … **Clause 4.2.4**: When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before the information can be used for that purpose. **Clause 4.3.1** Consent is required for the

	applicable qualification is justified. Where the Applicant answers **NO** and does not identify an applicable qualification the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the collection of their personal information must be provided.	collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified). **Clause 4.3.2** The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. **Clause 4.3.4** The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. **Clause 4.3.7** Individuals can give consent in many ways. For example: (*a*) an application form may be used to seek consent, collect information, and inform the individual of the

		use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses; (*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties; (*c*) consent may be given orally when information is collected over the telephone; or (*d*) consent may be given at the time that individuals use a product or service.
15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of mechanisms provided to individuals so that they may exercise choice in relation to the use of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be used.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. **Clause 4.2.3:** The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. … **Clause 4.2.4**: When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the

	Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent uses of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • being able to make use of the personal information, when the purposes of such use is not related or compatible to the purpose for which the information was collected, and • Personal information may be disclosed or distributed to third parties, other than Service Providers. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice, and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant a mechanism for individuals to exercise choice in relation to the use of their personal information must be provided.	individual is required before the information can be used for that purpose. **Clause 4.3.1** Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified). **Clause 4.3.2** The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. **Clause 4.3.3** An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes. **Clause 4.3.4** The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use,

		organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. **Clause 4.3.7** Individuals can give consent in many ways. For example: (*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses; (*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties; (*c*) consent may be given orally when information is collected over the telephone; or (*d*) consent may be given at the time that individuals use a product or service. **Clause 4.5** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant provides a description of how individuals may exercise choice in relation to the disclosure of their personal information, such as: • Online at point of collection • Via e-mail • Via preference/profile page • Via telephone • Via postal mail, or • Other (in case, specify) The Accountability Agent must verify that these types of mechanisms are in place and operational and identify the purpose(s) for which the information will be disclosed. Subject to the qualifications outlined below, the opportunity to exercise choice should be provided to the individual at the time of collection, for subsequent disclosures of personal information. Subject to the qualifications outlined below, the opportunity to exercise choice may be provided to the individual after collection, but before: • disclosing the personal information to third parties, other than Service Providers, for a purpose that is not related or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, or compatible with that for which	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2** The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected. **Clause 4.2.3:** The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. … **Clause 4.2.4**: When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before the information can be used for that purpose. **Clause 4.3.1** Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

	the information was collected. Where the Applicant answers **NO**, the Applicant must identify the applicable qualification to the provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not identify an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism for individuals to exercise choice in relation to the disclosure of their personal information must be provided.	**Clause 4.3.2** The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. **Clause 4.3.3** An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes. **Clause 4.3.4** The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. **Clause 4.3.7** Individuals can give consent in many ways. For example: (*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses; (*b*) a checkoff box may

		be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties; (*c*) consent may be given orally when information is collected over the telephone; or (*d*) consent may be given at the time that individuals use a product or service. **Clause 4.5** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.
17. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is displayed in a clear and conspicuous manner. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not displayed in a clear and conspicuous manner, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clear and conspicuous in order to comply with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.3.2** The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. **Clause 4.3.7** Individuals can give consent in

		many ways. For example: (*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses; (*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties; (*c*) consent may be given orally when information is collected over the telephone; or (*d*) consent may be given at the time that individuals use a product or service.
18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is clearly worded and easily understandable. Where the Applicant answers **NO**, and/or when the Accountability Agent finds that the Applicant's choice mechanism is not clearly worded and easily understandable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be clearly worded and easily understandable in order to comply with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2.5** Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected. **Clause 4.3.2** The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can

		reasonably understand how the information will be used or disclosed. **Clause 4.3.7** Individuals can give consent in many ways. For example: (*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses; (*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties; (*c*) consent may be given orally when information is collected over the telephone; or (*d*) consent may be given at the time that individuals use a product or service.
19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant's choice mechanism is easily accessible and affordable. Where the Applicant answers **NO**, or when the Accountability Agent finds that the Applicant's choice mechanism is not easily accessible and affordable, the Accountability Agent must inform the Applicant that all mechanisms that allow individuals to exercise choice in relation to the collection, use, and/or disclosure of their personal information, must be easily accessible and affordable in order to comply with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.2.5** Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected. **Clause 4.3.2** The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the

		individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. **Clause 4.3.7** Individuals can give consent in many ways. For example: (*a*) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses; (*b*) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties; (*c*) consent may be given orally when information is collected over the telephone; or (*d*) consent may be given at the time that individuals use a product or service.
20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.	Where the Applicant does have mechanisms in place, the Accountability Agent must require the Applicant to provide of the relevant policy or procedures specifying how the preferences expressed through the choice mechanisms (questions 14, 15 and 16) are honored. Where the Applicant does not have mechanisms in place, the Applicant must identify the applicable qualification to the	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; …

	provision of choice and provide a description and the Accountability Agent must verify whether the applicable qualification is justified. Where the Applicant answers **NO** and does not provide an acceptable qualification, the Accountability Agent must inform the Applicant that a mechanism to ensure that choices, when offered, can be honored, must be provided.	**Clause 4.3.1** Consent is required for the collection of personal information and the subsequent use or disclosure of this information. … **Clause 4.3.2** The principle requires "knowledge and consent". Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. **Clause 4.3.3** An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes. **Clause 4.5** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - *The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy*)**
21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use. The Accountability Agent will verify that reasonable procedures are in place to allow the Applicant to maintain personal information that is up to date, accurate and complete, to the extent necessary for the purpose of use. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.6** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. **Clause 4.6.1** The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual **Clause 4.6.2** An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected.

		Clause 4.6.3 Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.
22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures and steps the Applicant has in place for correcting inaccurate, incomplete and out-dated personal information, which includes, but is not limited to, procedures which allows individuals to challenge the accuracy of information such as accepting a request for correction from individuals by e-mail, post, phone or fax, through a website, or by some other method. The Accountability Agent must verify that this process is in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures/steps to verify and ensure that the personal information held is up to date, accurate and complete, to the extent necessary for the purposes of use, are required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; … **Clause 4.6** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. **Clause 4.6.2** An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected. **Clause 4.6.3** Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

		Clause 4.9.5 When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question. **Clause 4.9.6** When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.
23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred and the accompanying procedures to ensure that the corrections are also made by the processors, agents or other service providers acting on the Applicant's behalf. The Accountability Agent must verify that these procedures are in place and operational, and that they effectively ensure that	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; … **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been

	corrections are made by the processors, agents or other service providers acting on the Applicant's behalf. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to personal information processors, agent, or other service providers to whom the personal information was transferred, are required for compliance with this principle.	transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. **Clause 4.6** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. **Clause 4.6.1 …** Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual **Clause 4.6.2** An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected. **Clause 4.6.3** Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.
24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to communicate corrections to other third parties, to whom	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5**

third parties to whom the personal information was disclosed? If YES, describe.	personal information was disclosed. The Accountability Agent must verify that these procedures are in place and operational. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to communicate corrections to other third parties to whom personal information was disclosed, are required for compliance with this principle.	**Schedule 1:** **Clause 4.1** An organization is responsible for information under its control … **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; … **Clause 4.6** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. **Clause 4.6.1 …** Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual **Clause 4.6.2** An organization shall not routinely update personal information, unless such a process is necessary to fulfil the purposes for which the information was collected. **Clause 4.6.3** Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

25. Do you require personal information processors, agents, or other service providers acting on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?	Where the Applicant answers **YES**, the Accountability Agent must require the Applicant to provide the procedures the Applicant has in place to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed to ensure that personal information processors, agents, or other service providers to whom personal information was transferred inform the Applicant about any personal information known to be inaccurate incomplete, or outdated. The Accountability Agent will ensure that the procedures are in place and operational, and, where appropriate, lead to corrections being made by the Applicant and by the processors, agents or other service providers. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that procedures to receive corrections from personal information processors, agents, or other service providers to whom personal information was transferred or disclosed, are required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1** An organization is responsible for information under its control … **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; … **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. **Clause 4.6** Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used. **Clause 4.6.3** Personal information that is used on an ongoing basis, including information that is disclosed to third parties, should generally be accurate and up-to-date, unless limits to the requirement for accuracy are clearly set out.

SECURITY SAFEGUARDS

Assessment Purpose - *The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses*

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy*)**
26. Have you implemented an information security policy?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of this written policy. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that the implementation of a written information security policy is required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; … **Clause 4.5.3** Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. **Clause 4.7**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. **Clause 4.7.1**: The security safeguards shall protect the personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Organizations shall protect personal

		information regardless of the format in which it is held.
27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify the existence of such safeguards, which may include: • Authentication and access control (eg password protections) • Encryption • Boundary protection (eg firewalls, intrusion detection) • Audit logging • Monitoring (eg external and internal audits, vulnerability scans) • Other (specify) The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information and/or Third Party personal information it collects, in order to protect that information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. Such safeguards must be proportional to the	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; … **Clause 4.5.3** Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. **Clause 4.7**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. **Clause 4.7.1**: The security safeguards shall protect the personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Organizations shall protect personal information regardless of the format in which it is held. **Clause 4.7.3** The methods of protection

	probability and severity of the harm threatened the sensitivity of the information, and the context in which it is held. The Applicant must take reasonable measures to require information processors, agents, contractors, or other service providers to whom personal information is transferred to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness. Where the Applicant indicates that it has **NO** physical, technical and administrative safeguards, or inadequate safeguards, to protect personal information, the Accountability Agent must inform the Applicant that the implementation of such safeguards is required for compliance with this principle.	should include (*a*) physical measures, for example, locked filing cabinets and restricted access to offices; (*b*) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (*c*) technological measures, for example, the use of passwords and encryption. **Clause 4.7.5** Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3)
28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.	Where the Applicant provides a description of the physical, technical and administrative safeguards used to protect personal information, the Accountability Agent must verify that these safeguards are proportional to the risks identified. The Applicant must implement reasonable administrative, technical and physical safeguards, suitable to the Applicant's size and complexity, the nature and scope of its activities, and the confidentiality or sensitivity of the personal information (whether collected directly from the individuals or through a third	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; … **Clause 4.7**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

	party) it gathers, in order to protect that information from unauthorized leakage, loss, use, alteration, disclosure, distribution, or access.	**Clause 4.7.2**: The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information and the method of storage. More sensitive information should be safeguarded by a higher level of protection.
29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).	The Accountability Agent must verify that the Applicant's employees are aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight as demonstrated by procedures, which may include: • Training program for employees • Regular staff meetings or other communications • Security policy signed by employees • Other (specify) Where the Applicant answers that it does not make employees aware of the importance of, and obligations respecting, maintaining the security of personal information through regular training and oversight, the Accountability Agent has to inform the Applicant that the existence of such procedures are required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (*a*) implementing procedures to protect personal information; (*c*) training staff and communicating to staff information about the organization's policies and practices; … **Clause 4.5.3** Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. **Clause 4.7**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. **Clause 4.7.4** Organizations shall make their employees aware of the importance of

		maintaining the confidentiality of personal information.
30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through: 30.a) Employee training and management or other safeguards? 30.b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal? 30.c) Detecting, preventing, and responding to attacks, intrusions, or other security failures? 30.d) Physical security?	Where the Applicant answers **YES** (to questions 30.a to 30.d), the Accountability Agent has to verify the existence each of the safeguards. The safeguards have to be proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held. The Applicant must employ suitable and reasonable means, such as encryption, to protect all personal information. Where the Applicant answers **NO** (to questions 30.a to 30.d), the Accountability Agent must inform the Applicant that the existence of safeguards on each category is required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.5.3** Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. **Clause 4.7**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. **Clause 4.7.1**: The security safeguards shall protect the personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Organizations shall protect personal information regardless of the format in which it is held. **Clause 4.7.2**: The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information and the method of storage. More sensitive information should be safeguarded

		by a higher level of protection. **Clause 4.7.3** The methods of protection should include (*a*) physical measures, for example, locked filing cabinets and restricted access to offices; (*b*) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (*c*) technological measures, for example, the use of passwords and encryption. **Clause 4.7.4** Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information. **Clause 4.7.5** Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3)
31. Have you implemented a policy for secure disposal of personal information?	Where the Applicant answers **YES**, the Accountability Agent must verify the implementation of a policy for the secure disposal of personal information. Where the Applicant answers **NO**, the Accountability Agent must inform Applicant that the existence of a policy for the secure disposal of personal information is required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (*a*) implementing procedures to protect personal information; **Clause 4.5.3** Personal information that is no

		longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. **Clause 4.7**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. **Clause 4.7.1**: The security safeguards shall protect the personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Organizations shall protect personal information regardless of the format in which it is held. **Clause 4.7.5** Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).
32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures. Where the Applicant answers **NO,** the Accountability Agent must inform the Applicant that the existence of measures to detect, prevent, and respond to attacks, intrusions, or other security failures, is required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; …

		Clause 4.5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. **Clause 4.7**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. **Clause 4.7.1**: The security safeguards shall protect the personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Organizations shall protect personal information regardless of the format in which it is held. **Clause 4.7.3** The methods of protection should include (*a*) physical measures, for example, locked filing cabinets and restricted access to offices; (*b*) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (*c*) technological measures, for example, the use of passwords and encryption.
33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.	The Accountability Agent must verify that such tests are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these tests.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:**

		Clause 4.7.1: The security safeguards shall protect the personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Organizations shall protect personal information regardless of the format in which it is held. **Clause 4.7.3** The methods of protection should include (*a*) physical measures, for example, locked filing cabinets and restricted access to offices; (*b*) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (*c*) technological measures, for example, the use of passwords and encryption.
34. Do you use risk assessments or third-party certifications? Describe below.	The Accountability Agent must verify that such risk assessments or certifications are undertaken at appropriate intervals, and that the Applicant adjusts their security safeguards to reflect the results of these certifications or risk assessments. One example is whether privacy compliance audits are carried out by the Applicant and if audits are carried out, the Accountability Agent must verify whether recommendations made in the audits are implemented.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; … **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to

		provide a comparable level of protection while the information is being processed by a third party. **Clause 4.7.3** The methods of protection should include (*a*) physical measures, for example, locked filing cabinets and restricted access to offices; (*b*) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (*c*) technological measures, for example, the use of passwords and encryption.
35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by: 35.a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided? 35.b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of the personal information of the Applicant's customers? 35.c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?	The Accountability Agent must verify that the Applicant has taken reasonable measures (such as by inclusion of appropriate contractual provisions) to require information processors, agents, contractors, or other service providers to whom personal information is transferred, to protect against leakage, loss or unauthorized access, destruction, use, modification or disclosure or other misuses of the information. The Applicant must periodically review and reassess its security measures to evaluate their relevance and effectiveness.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; … **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

		Clause 4.5.3 Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information. **Clause 4.7**: Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. **Clause 4.7.1**: The security safeguards shall protect the personal information against loss or theft, as well as unauthorized access, disclosure, copying, use or modification. Organizations shall protect personal information regardless of the format in which it is held. **Clause 4.7.2**: The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information and the method of storage. More sensitive information should be safeguarded by a higher level of protection. **Clause 4.7.3** The methods of protection should include (*a*) physical measures, for example, locked filing cabinets and restricted access to offices; (*b*) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and (*c*) technological measures, for example, the

		use of passwords and encryption. **Clause 4.7.4** Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information. **Clause 4.7.5** Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3)

ACCESS AND CORRECTION

Assessment Purpose - *The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.*

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. Section II of the CBPR Self-Assessment Guidelines for Organisations sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy*)**
36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures in place to respond to such requests. The Applicant must grant access to any individual, to personal information collected or gathered about that individual, upon receipt of sufficient information confirming the individual's identity. The Applicant's processes or mechanisms for access by individuals to personal information must be reasonable having regard to the manner of request and the nature of the personal information. The personal information must be provided to	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.9** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. **Clause 4.9.1** Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged

	individuals in an easily comprehensible way. The Applicant must provide the individual with a time frame indicating when the requested access will be granted. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed. **Clause 4.9.2** An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose. **Clause 4.9.3** In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual. **Clause 4.9.4** An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be

		provided.
37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your applicant's policies/procedures for receiving and handling access requests. Where NO, proceed to question 38. 37.a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe. 37.b) Do you provide access within a reasonable time frame following an individual's request for access? If YES, please describe. 37.c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe. 37.d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)? 37.e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee	Where the Applicant answers **YES** the Accountability Agent must verify each answer provided. The Applicant must implement reasonable and suitable processes or mechanisms to enable the individuals to access their personal information, such as account or contact information. If the Applicant denies access to personal information, it must explain to the individual why access was denied, and provide the appropriate contact information for challenging the denial of access where appropriate. Where the Applicant answers **NO** and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that it may be required to permit access by individuals to their personal information. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.9** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate. **Clause 4.9.1** Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed. **Clause 4.9.2** An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal

is not excessive.		information. The information provided shall only be used for this purpose. **Clause 4.9.3** In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual. **Clause 4.9.4** An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.
38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your applicant's policies/procedures in this regard below and answer questions 37 (a), (b), (c), (d) and (e). 38.a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if	Where the Applicant answers **YES to questions 38a to 38e**, the Accountability Agent must verify that such policies are available and understandable in the primarily targeted economy. If the Applicant denies correction to the individual's personal information, it must explain to the individual why the correction request was denied, and provide the appropriate contact information for challenging the denial of correction where appropriate.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.9** Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information

necessary. 38.b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion? 38.c) Do you make such corrections or deletions within a reasonable time frame following an individual's request for correction or deletion? 38.d) Do you provide a copy to the individual of the corrected personal information or provide confirmation that the data has been corrected or deleted? 38.e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?	All access and correction mechanisms have to be simple and easy to use, presented in a clear and visible manner, operate within a reasonable time frame, and confirm to individuals that the inaccuracies have been corrected, amended or deleted. Such mechanisms could include, but are not limited to, accepting written or e-mailed information requests, and having an employee copy the relevant information and send it to the requesting individual. Where the Applicant answers **NO** to questions 38a-38e and does not identify an applicable qualification, the Accountability Agent must inform the Applicant that the existence of written procedures to respond to such requests is required for compliance with this principle. Where the Applicant identifies an applicable qualification, the Accountability Agent must verify whether the applicable qualification is justified.	and have it amended as appropriate. **Clause 4.9.5** When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question. **Clause 4.9.6** When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question **Clause 4.10** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance. **Clause 4.1.2** The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request. **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including … establishing procedures to receive and respond to

		complaints and inquiries.

ACCOUNTABILITY

Assessment Purpose - *The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent.*

Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.

Question (*to be answered by the Applicant*)	**Assessment Criteria (*to be verified by the Accountability Agent*)**	**Enforceability (*to be answered by the Economy*)**
39. What measures do you take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe. • Internal guidelines or policies (if applicable, describe how implemented) __ • Contracts ___ • Compliance with applicable industry or sector laws and regulations __ • Compliance with self- regulatory applicant code and/or rules ___ • Other (describe) __	The Accountability Agent has to verify that the Applicant indicates the measures it takes to ensure compliance with the APEC Information Privacy Principles.	***Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles. **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being

		processed by a third party. **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (*a*) implementing procedures to protect personal information; (*b*) establishing procedures to receive and respond to complaints and inquiries; (*c*) training staff and communicating to staff information about the organization's policies and practices; and (*d*) developing information to explain the organization's policies and procedures.
40. Have you appointed an individual(s) to be responsible for your overall compliance with the Privacy Principles?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has designated an employee(s) who is responsible for the Applicant's overall compliance with these Principles. The Applicant must designate an individual or individuals to be responsible for the Applicant's overall compliance with privacy principles as described in its Privacy Statement, and must implement opportune procedures to receive, investigate, and respond to privacy-related complaints, providing an explanation of any remedial action where applicable. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that designation of such an employee(s) is required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1** An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles. **Clause 4.1.1** Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

		Clause 4.1.2 The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.
41. Do you have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to receive, investigate and respond to privacy-related complaints, such as: 1) A description of how individuals may submit complaints to the Applicant (e.g. Email/Phone/Fax/Postal Mail/Online Form); AND/OR 2) A designated employee(s) to handle complaints related to the Applicant's compliance with the APEC Privacy Framework and/or requests from individuals for access to personal information; AND/OR 3) A formal complaint-resolution process; AND/OR 4) Other (must specify). Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.10** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance. **Clause 4.10.2** Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use. **Clause 4.10.3** Organizations shall inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures. A range of these procedures may exist. For example, some regulatory bodies accept complaints about the personal-information handling practices of the companies they regulate. **Clause 4.10.4** An organization shall

		investigate all complaints. If a complaint is found to be justified, the organization shall take appropriate measures, including, if necessary, amending its policies and practices.
42. Do you have procedures in place to ensure individuals receive a timely response to their complaints?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place to ensure individuals receive a timely response to their complaints. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such procedures is required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.10** An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance. **Clause 4.10.2** Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.
43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.	The Accountability Agent must verify that the Applicant indicates what remedial action is considered.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; (b) establishing procedures to receive and respond

		to complaints and inquiries; … **Clause 4.10.2** Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.
44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify that the Applicant has procedures regarding training employees with respect to its privacy policies and procedures, including how to respond to privacy-related complaints. Where the Applicant answers that it does not have procedures regarding training employees with respect to their privacy policies and procedures, including how to respond to privacy-related complaints, the Accountability Agent must inform the Applicant that the existence of such procedures is required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; (b) establishing procedures to receive and respond to complaints and inquiries; (c) training staff and communicating to staff information about the organization's policies and practices; (d) developing information to explain the organization's policies and procedures.
45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?	Where the Applicant answers **YES,** the Accountability Agent must verify that the Applicant has procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information, as well as provide the necessary training to employees regarding this subject. Where the Applicant answers **NO**, the	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Part 1 – Division 1: Protection of Personal Information** **Subsection 7. (1)** For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may

	Accountability Agent must inform the Applicant that such procedures are required for compliance with this principle.	collect personal information without the knowledge or consent of the individual only if … (e) the collection is made for the purpose of making a disclosure … (ii) that is required by law. **Subsection 7(2)** For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if … (d) it was collected under paragraph (1)…(e) **Subsection 7(3)** For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is … (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records; …; or (i) required by law.
46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)? • Internal guidelines or policies __	Where the Applicant answers **YES,** the Accountability Agent must verify the existence of each type of agreement described. Where the Applicant answers **NO**, the Accountability Agent must inform the Applicant that implementation of such agreements is required for compliance with this principle.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (*a*) implementing

• Contracts __ • Compliance with applicable industry or sector laws and regulations __ • Compliance with self- regulatory applicant code and/or rules __ • Other (describe) __		procedures to protect personal information; **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
47. Do these agreements generally require that personal information processors, agents, contractors or other service providers: • Abide by your APEC- compliant privacy policies and practices as stated in your Privacy Statement? __ • Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? __ • Follow instructions provided by you relating to the manner in which your personal information must be handled? __ • Impose restrictions on subcontracting unless with your consent? __ • Have their CBPRs certified by an APEC accountability agent in their jurisdiction? __ • Notify the Applicant in the case of a breach of the personal information of the Applicant's	The Accountability Agent must verify that the Applicant makes use of appropriate methods to ensure their obligations are met.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (*a*) implementing procedures to protect personal information; **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

customers? __ • Other (describe)		
48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.	The Accountability Agent must verify the existence of such self-assessments.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (*a*) implementing procedures to protect personal information; **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other services providers to ensure compliance with your instructions and/or agreements/contracts? If yes, describe.	Where the Applicant answers **YES**, the Accountability Agent must verify the existence of the Applicant's procedures such as spot checking or monitoring mechanisms. Where the Applicant answers **NO**, the Accountability Agent must require the Applicant to describe why it does not make use of such spot checking or monitoring mechanisms.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Schedule 1:** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (*a*) implementing procedures to protect personal information; **Clause 4.1.3** An organization is responsible for personal information in its possession or

		custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.
50. Do you disclose personal information to other recipient persons or organizations in situations where due diligence and reasonable steps to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?	If **YES**, the Accountability Agent must ask the Applicant to explain: (1) why due diligence and reasonable steps consistent with the above Assessment Criteria for accountable transfers are impractical or impossible to perform; and (2) the other means used by the Applicant for ensuring that the information, nevertheless, is protected consistent with the APEC Privacy Principles. Where the Applicant relies on an individual's consent, the Applicant must explain to the satisfaction of the Accountability Agent the nature of the consent and how it was obtained.	***Personal Information Protection and Electronic Documents Act*** **(PIPEDA), S.C. 2000, c.5** **Part 1 – Division 1: Protection of Personal Information** **S. 5(1)** Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1 **Schedule 1** **Clause 4.1.4** Organizations shall implement policies and practices to give effect to the principles, including (*a*) implementing procedures to protect personal information; **Clause 4.1.3** An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.