Privacy Conformance Profile Discussion Draft Version 0.12

This Discussion Draft has been developed by the Digital ID & Authentication Council of Canada (DIACC) Trust Framework Expert Committee (TFEC). The TFEC operates under the controlling policies of the DIACC. Comments submitted by the public are subject to the DIACC Contributor Agreement.

DIACC expects to modify and improve this Discussion Draft based upon public comments. The purpose of the open commentary is to ensure transparency in development and diversity of a truly Pan-Canadian input. Comments made during the review will be considered for incorporation to the next draft. DIACC will prepare a disposition of comments to provide transparency with regard to how each comment was handled.

Forthcoming PCTF releases will expand, clarify, and refine the content of this document. The intended target audience is inclusive of decision makers who may or may not be domain technology experts.

When reviewing this draft, please consider the following:

1. Is the general structure and tone appropriate for covering Privacy in the context of digital identity?
2. Do the documents strike an appropriate balance between elaborating privacy requirements for digital identity aligned with the PIPEDA principles and not being redundant with what PIPEDA says?
3. Are the conformance criteria sufficiently clear and unambiguous that you could apply them in your context?
4. Does the distinction between a Subject's Personal Information and Service Information make sense and/or apply in your context?

Notes:

- Governance of Privacy and other PCTF components are part of ongoing discussions. Comments from this review concerning governance will be referred to the PCTF Governance Design Team.
- Privacy-related requirements specific to notice and consent processes are detailed in the PCTF "Notice and Consent" component.

Table of Contents

1 Introduction to the Privacy Conformance Profile

The Conformance Criteria for the Privacy Component specify how the PIPEDA Fair Information Principles, defined by the Office of the Privacy Commissioner of Canada, are relevant/apply to the handling of digital identity data. (Note: These do not intend to replace existing regulations; organizations are expected to meet privacy regulations in their jurisdiction.)

1.1 Relationship to the Pan-Canadian Trust Framework

The Pan-Canadian Trust Framework (PCTF) consists of a set of modular or functional components that can be independently assessed and certified for consideration as trusted components. Building on a Pan-Canadian approach, the PCTF enables the public and private sector to work collaboratively to safeguard digital identities by standardizing processes and practices across the Canadian digital ecosystem.

Figure 1 is an illustration of the Pan-Canadian Trust Framework Model Visual Draft. The Privacy Component is relevant to all sub-components.

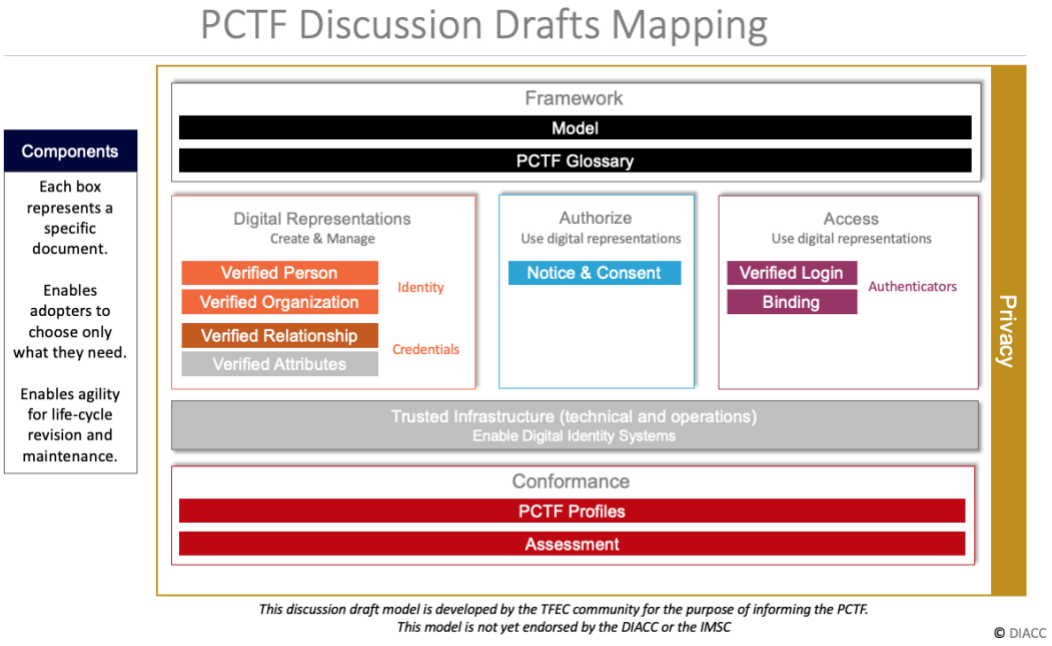

Figure 1. Pan-Canadian Trust Framework Model Visual Draft

1.2 Keywords

To ensure consistent application, keywords that appear in **bold** in the conformance criteria are to be interpreted as follows:

- **MUST** means that the requirement is absolute as part of the conformance criteria.
- **MUST NOT** means that the requirement is an absolute prohibition of the conformance criteria.
- **SHOULD** means that while there may exist valid reasons in particular circumstances to ignore the requirement, the full implications must be understood and carefully weighed before not choosing to adhere to the conformance criteria or choosing a different option as specified by the conformance criteria.
- **SHOULD NOT** means that valid reason may exist in particular circumstances when the requirement is acceptable or even useful, however, the full implications should be understood and the case carefully weighed before choosing to not conform to the requirement as described.
- **MAY** means that the requirement is discretionary but recommended.

Additional keywords, such as normative definitions in related standards and specification, will also be indicated in **bold**.

1.3 Definitions

Two types of Personal Information are defined:

- **Service Information –** information collected or generated by the participants (Disclosing Organization, Requesting Organization, Notice and Consent Processor(s), or Network Provider) for purposes of operating and maintaining the service (e.g., service specific pseudonymous identifiers, transaction records, proofs of transactions including consent).
- **Subject's Personal Information –** information that a Subject consents to share from a Disclosing Organization to a Requesting Organization (e.g., name, email address, phone number, mailing address, date of birth, account information).

1.4 Roles

The following roles are defined to cover the scope of the Privacy Component. Depending on the use case, separate organizations may take on one or more roles.

- **Digital Identity Ecosystem –** A set of public and private sector organizations (e.g., government, commercial, non-profit, and other entities) who offer and consume digital identity services and agree to comply with a common set of conformance criteria for their business and technical processes when exchanging digital identity information to ensure trustworthy digital transactions.
- **Disclosing Organization –** the organization that currently holds the Subject's Personal Information, that the Subject consents to disclose to a Requesting Organization. In a digital identity context, this will often be an identity or attribute provider.

- **Governing Body –** the organization that oversees the trust framework and the associated requirements of the digital identity ecosystem. This could involve providing governance as well as business, technical or commercial arrangements between the parties of the transaction.
- **Notice and Consent Processor –** the organization that provides the notice to the Subject of the request for Personal Information (from the Requesting Organization), obtains and records the consent and provides the Subject with the means to manage the consent going forward, including the withdrawal of consent.
- **Network Provider –** the organization that connects the parties together in a multi-party identity transaction. This organization is an active participant and adds value in the delivery of the digital identity service (e.g., not an internet service provider that passively provides internet connectivity).
- **Requesting Organization –** the organization that the Subject consents to disclose Personal Information to. In a digital identity context, this will often be a service provider or relying party.
- **Subject –** natural person to whom the Personal Information in question pertains. (Note: Delegated Authority is not addressed in this document).

These roles help to isolate the different functions and responsibilities within the end-to-end privacy processes. They are not intended to imply any particular solution, architecture or implementation.

For example, in some cases, the notice may be presented and consent collected from an organization facilitating Personal Information exchange between the Subject, Disclosing Organization and Requesting Organization. In other cases, the notice may be presented and consent collected directly by either the Disclosing or Requesting Organization, in which case that organization would also be the Notice and Consent Processor.

2 Trusted Principles and Conformance Criteria

The conformance criteria listed below are organized and intended to align with the Office of the Privacy Commissioner of Canada's PIPEDA fair information principles. For ease of reference, a specific conformance criteria may be referred by its category and reference no. (e.g., "**BASE-1**" refers to "Baseline Conformance Criteria Reference No. 1").

Reference	Conformance Criteria
BASE	**Baseline** **Note:** Requirements for use cases where the Subject acts as the Disclosing Organization are not addressed in this version of the Baseline conformance criteria.
1	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Providers and the Governing Body **MUST** have a privacy management program in place to ensure legal compliance including the implementation of privacy policies, practices, controls and assessment tools.

133	2	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Providers and the Governing Body **MUST** have a Privacy Officer or similar position in place who is responsible for overseeing the privacy management program and any internal audits or reviews of personal information handling practices (including those related to the provision of notice and the obtaining of consent).
134	3	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Providers and the Governing Body **MUST** have a comprehensive privacy policy that: • provides a description of its personal information handling practices; and • is easily accessible, simple to read, and updated as required.
135	4	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Providers and the Governing Body **MUST** periodically audit or review their personal information management practices (including its notice and consent management practices) to ensure that Personal Information is being handled in the way described by its privacy policy.
136	5	The Governing Body **MUST** ensure organizations operating within the Digital Identity Ecosystem are following Principles 1-10.
137	6	As part of their privacy management programs, Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Providers and the Governing Body **MUST** have processes to manage personal information breaches, which includes reporting, containment, remediation, and prevention steps.
138	**ACCO**	**Principle 1 - Accountability** *An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.*
139	1	Disclosing Organizations, Requesting Organizations, Network Providers, and Notice and Consent Processors **MUST** ensure the Subject has a clear idea of who is responsible for privacy in their respective organizations. Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** provide the name or title of that person to the Subject and provide them with the means to contact that person.

140	2	The Disclosing Organization **MUST** have a privacy management program that includes: • restrictions on types of organizations with whom the Subject's Personal Information will be shared, for example, based on sector or regulatory environment (e.g., health, financial services); • If applicable, specification of the requirements to be met by relevant Digital Identity Ecosystem participants regarding the handling of a Subject's Personal Information; • restrictions on the process of sharing the Subject's Personal Information, for example, the level of assurance needed; • processes to be followed when the Subject's Personal Information is shared; • processes to be followed when the Subject's Personal Information previously shared is updated, deleted or expired; • clear guidance for Subjects on the sharing of the Subject's Personal Information to help them know which party they should contact depending on the nature of their inquiry; and • privacy impact assessment that explicitly covers the sharing of the Subject's Personal Information through the Digital Identity Ecosystem.
141	3	The Disclosing Organization **MUST** ensure that the responsibilities of their designated privacy official include the authority to intervene on privacy issues specifically relating to the organization's role as a Disclosing Organization. This will ensure a holistic and consistent approach to the protection of the Subject's privacy.
142	4	The Requesting Organization **MUST** have a privacy management program that includes: • restrictions on types of organizations from whom the Subject's Personal Information will be obtained, for example, based on sector, regulatory environment (e.g., health, financial services); • If applicable, processes to be followed by the Requesting Organization to comply with specific requirements defined by a Disclosing Organization on the Subject's Personal Information; • restrictions on the process of obtaining the Subject's Personal Information, for example, the level of assurance needed; • processes to be followed when the Subject's Personal Information is obtained via the digital identity system; • processes to be followed when the Subject's Personal Information previously obtained is updated, deleted or expired; • clear guidance for Subjects on the sharing of data to help them know which party they should contact depending on the nature of their inquiry; and • privacy impact assessment that explicitly covers the use of the Subject's Personal Information obtained through the Digital Identity Ecosystem.
143	5	The Requesting Organization **MUST** ensure that the responsibilities of their designated privacy official include the authority to intervene on privacy issues specifically relating to the organization's role as a Requesting Organization. This will ensure a holistic and consistent approach to the protection of the Subject's privacy.

144	6	The Notice and Consent Processor **MUST** have a privacy management program that includes: • restrictions on use of Personal Information where the Notice and Consent Processor is just a facilitator, for example, potentially the Notice and Consent Processor should never be in possession of or store the Subject's Personal Information; • If applicable, processes to be followed by the Notice & Consent Processor to comply with specific requirements defined by a Disclosing Organization on the Subject's Personal Information; • processes to be followed when facilitating the sharing of the Subject's Personal Information; • processes to be followed when the Subject's Personal Information previously shared is updated, deleted or expired; • clear guidance for Subjects on the sharing of the Subject's Personal Information to help them know which party they should contact depending on the nature of their inquiry; and • privacy impact assessment that explicitly covers the facilitation role, focusing on minimizing (or even eliminating) access to or visibility of the Subject's Personal Information or Service Information.
145	7	The Notice and Consent Processor **MUST** ensure that the responsibilities of their designated privacy official include the authority to intervene on privacy issues specifically relating to the organization's role as a Notice and Consent Processor. This will ensure a holistic and consistent approach to the protection of the Subject's privacy.
146	8	The Network Provider **MUST** have a privacy management program that includes: • restrictions on use of Personal Information where the Network Provider is just a facilitator, for example, potentially the Network Provider should never be in possession of or store the Subject's Personal Information; • processes to be followed when facilitating the sharing of the Subject's Personal Information; • processes to be followed when the Subject's Personal Information previously shared is updated, deleted or expired; • clear guidance for Subjects on the sharing of the Subject's Personal Information to help them know which party they should contact depending on the nature of their inquiry; and • privacy impact assessment that explicitly covers the facilitation role, focusing on minimizing (or even eliminating) access to or visibility of the Subject's Personal Information or Service Information.

147	9	The Governing Body **MUST** have end-to-end governance arrangements in place that: • ensure accountability of the organizations operating with the digital identity ecosystem; • If applicable, ensure that specific requirements defined by an organization on a Subject's Personal Information are complied with by relevant digital identity ecosystem participants; • include rules concerning standards and interoperability that ensure all parties in the sharing of the Subject's Personal Information treat the Subject and the Subject's Personal Information in a consistent and compatible way; • include procedures to investigate and manage privacy breaches, including assessing the risk to individuals and reporting breaches to regulators and individuals; and • facilitate fraud monitoring across the digital identity ecosystem, including data sharing arrangements for the purposes of monitoring fraud.
148	**IDEN**	**Principle 2 - Identifying Purposes** *The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.*
149	1	The Disclosing Organization **MUST** have confidence that Principle 2 is being followed by Requesting Organizations and Notice and Consent Processors before disclosing Personal Information to those organizations.
150	2	The Disclosing Organization **MUST** maintain and preserve a timeline of retrievable documentation for records of information requests and disclosure events. The timeline may consist of a single event (a "one time request and disclosure"), or multiple events depending on the circumstances of the exchange.
151	3	The Requesting Organization must clearly identify the purpose for collecting Subject's Personal Information through the Notice and Consent Processor.
152	4	The Requesting Organization **MUST** maintain and preserve a timeline of retrievable documentation for why Personal Information is needed and how it will be used.
153	5	The Requesting Organization **MUST** periodically perform an internal review of their Personal Information collection and use requirements, and update future requests accordingly.
154	6	The Requesting Organization **MUST** ensure that the reasons for the collection and use of information to be clear, unambiguous, and not overly broad.
155	7	Before or when any Personal Information is collected, the Notice and Consent Processor **MUST** explain in writing to the Subject why it is needed and how it will be used.
156	8	The Governing Body **MUST** be clearly define the scope of the Digital Identity Ecosystem to all participants and that identifying purposes beyond the scope of the Digital Identity Ecosystem (which may exist within each participating organization) are not covered.
157	9	The Governing Body **MUST** ensure that organizations operating within the Digital Identity Ecosystem are following Principle 2.

158	10	The Governing Body **MUST** include procedures to investigate and manage deviations from Principle 2, including assessing the risk to Subjects and reporting of breaches to regulators and Subjects.
159	**CONS**	**Principle 3 - Consent** *The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.*
160	1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the notice and consent request is clear, understandable and meaningful to the Subject.
161	2	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** ensure the consent process balances sufficient information to the Subject against information overload. In all cases, a straightforward means **SHOULD** be provided for the Subject to get additional information, as may be required.
162	3	The Disclosing Organization **MUST** ensure the Notice and Consent Processor performs its function appropriately prior to disclosing the Subject's Personal Information.
163	4	The Disclosing Organization **MUST** ensure that sufficient evidence of the notice and consent is obtained from the Notice and Consent Processor and then stored appropriately.
164	5	The Disclosing Organization **MUST** confirm consent is valid (i.e., not expired or revoked) at the time of sharing a Subject's Personal Information. In the event that consent is not valid, Disclosing Organization's **MUST** provide a proper response to the Requesting Organization.
165	6	The Disclosing Organization **MUST** ensure the Subject understands the nature, purpose, and consequences of the collection, use or disclosure of the Subject's Personal Information to which they are consenting.
166	7	The Requesting Organization is the originator of the request for consent and hence **MUST** be primarily responsible for determining the content of the notice.
167	8	The Requesting Organization **SHOULD** ensure that the request follows a principle of minimal disclosure.
168	9	The Requesting Organization **MUST** ensure the Notice and Consent Processor performs its function appropriately prior to receiving Subject's Personal Information.
169	10	The Requesting Organization **MUST** ensure that sufficient evidence of the notice and consent is obtained from the Notice and Consent Processor and then stored appropriately.
170	11	Requesting Organization **SHOULD** properly handle revocation of subscription type consent via the digital identity ecosystem.
171	12	The Notice and Consent Processor **MUST** be responsible for providing notice to the Subject within the Digital Identity Ecosystem.

172	13	The Notice and Consent Processor **MUST** ensure notice is clearly reflecting the nature of sharing within the Digital Identity Ecosystem.
173	14	The Notice and Consent Processor **MUST** ensure that the Subject is authenticated prior to displaying any Subject's Personal Information within a notice to the Subject by validating the identity of the Subject.
174	15	The Notice and Consent Processor **MUST** provide a means to collect consent and communicate this to the other parties involved in the digital identity transaction (Disclosing Organization and Requesting Organization).
175	16	The Notice and Consent Processor **MUST** record the consent and provide the Subject with means to review and manage any consents given.
176	17	For identity transactions where consent is being managed between multiple Requesting Organizations and Disclosing Organizations, the Notice and Consent Processor MUST ensure all organizational boundaries are maintained and/or preserved.
177	18	The Notice and Consent Processor **MUST** have processes in place to support the revocation of consent. This could originate from the Subject or be in response to a fraud being detected, for example.
178	19	The Network Provider **MAY** be involved in determining or discovering which Disclosing Organizations are potential sources of the requested Personal Information.
179	20	The Network Provider **SHOULD NOT** have visibility to unprotected Personal Information. This includes any Personal Information presented in the notice and consent process, as well as transmission of Personal Information through the network.
180	21	The Governing Body **SHOULD** provide guidelines on the formulation of notices and collection of consent, to provide a consistent and optimized user experience across the Digital Identity Ecosystem.
181	22	The Governing Body **MUST** ensure that organizations operating within the Digital Identity Ecosystem are following Principle 3.
182	23	The Governing Body **MUST** include procedures to investigate and manage deviations from Principle 3, including assessing the risk to Subjects and reporting breaches to regulators and Subjects.
183	**LIMC**	**Principle 4 - Limiting Collection** *The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.*
184	1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** ensure that only Personal Information that is necessary will be collected from the Subject.

185	2	The Disclosing Organization **MUST** have confidence that the Requesting Organization has good and sufficient reason for collecting the requested Personal Information.
186	3	The Requesting Organization **MUST** clearly delineate information collection activities via the Digital Identity Ecosystem from other activities of the Requesting Organization.
187	4	The Requesting Organization **MUST** limit the Personal Information that is collected via the Digital Identity Ecosystem to what is necessary for the specific purpose of using the Digital Identity Ecosystem, e.g., to allow Subjects to access services or prove entitlement.
188	5	Requirement removed (redundant with #4). Renumber in final version.
189	6	The Requesting Organization **MUST** publicly document the kind and purpose of Personal Information collected.
190	7	The Requesting Organization **MUST** ensure that staff members can explain the kind and purpose of Personal Information collected.
191	8	The Requesting Organization **MUST** be clear, unambiguous, and transparent about the reason for collecting Personal Information in all forms of communication.
192	9	The Notice and Consent Processor **MUST** ensure that Personal Information required to perform the Notice and Consent function is minimized.
193	10	The Network Provider **MUST** facilitate the sharing of Personal Information but **SHOULD NOT** have visibility of the Personal Information itself during the collection of protected Personal Information for the purpose of sharing.
194	11	The Governing Body **MUST** ensure that organizations operating within the Digital Identity Ecosystem are following Principle 4.
195	12	The Governing Body **MUST** have confidence that the Requesting Organization has good and sufficient reason for collecting the requested Personal Information.
196	13	The Governing Body **MUST** define rules and guidelines on appropriate ways to the limit collection of Personal Information within and by the Digital Identity Ecosystem participants.
197	14	The Governing Body **MUST** include procedures to investigate and manage deviations from Principle 4, including assessing the risk to Subjects and reporting breaches to regulators and Subjects.
198	**LIMU**	**Principle 5 - Limiting Use, Disclosure, and Retention** *Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.*
199	1	The Disclosing Organization **MUST** have internal policies and other documentation for limiting use, disclosure, and retention of Subject's Personal Information.
200	2	The Disclosing Organization **MUST** document uses of Subject's Personal Information for the purpose of disclosure within the Digital Identity Ecosystem.

201	3	In the event the there is a defined minimum and maximum data retention policy specified for the Digital Identity Ecosystem, the Disclosing Organization **MUST** account for that policy with respect to the Subject's Personal Information in connection with the digital identity ecosystem. Note: Subject to regulatory restrictions.
202	4	The Disclosing Organization **MUST** limit disclosure of the Subject's Personal Information to only that required for the specific and intended purpose in alignment with Subject's consent.
203	5	The Disclosing Organization **MUST** limit disclosure of the Subject's Personal Information to only that which the Disclosing Organization has confidence in the accuracy and currency of.
204	6	The Requesting Organization **MUST** document uses of Subject's Personal Information received via the Digital Identity Ecosystem.
205	7	The Requesting Organization **MUST** institute maximum and minimum valid retention periods of the Subject's Personal Information received via the Digital Identity Ecosystem.
206	8	The Requesting Organization **MUST NOT** use or retain, without obtaining proper consent, the Subject's Personal Information (received through the Digital Identity Ecosystem) for purposes other than that specified through the Notice and Consent Processor at the time of collection.
207	9	The Notice and Consent Processor **MUST** have internal policies and other documentation for limiting use, disclosure, and retention of Personal Information.
208	10	The Notice and Consent Processor **MUST** document the use of the Subject's Personal Information for the new purpose of providing notices and obtaining consents within the Digital Identity Ecosystem. Ideally, the Notice and Consent Processor would not have visibility of Personal Information, this is, however, dependent on both the implementation and the requirements to present the Subject's Personal Information itself as part of the consent process.
209	11	The Notice and Consent Processor **MUST** institute maximum and minimum valid retention periods of the Subject's Personal Information as they pertain to the Digital Identity Ecosystem.
210	12	The Notice and Consent Processor **MUST** dispose of Personal Information that is no longer required for the digital identity-related purpose for which it was retained.
211	13	The Personal Information that the Subject is consenting to share with a Requesting Organization(s) **MUST NOT** flow from the Notice and Consent Processor to any organization other than the Requesting Organization(s) identified in the consent. This includes the Notice and Consent Processor itself, with the exception of information to authenticate the Subject.
212	14	The Network Provider **MUST** facilitate the sharing of Personal Information but **SHOULD NOT** have visibility of the Personal Information itself during the collection of protected Personal Information for the purpose of sharing.

213	15	The Governing Body **MUST** define rules for the end-to-end use, disclosure, and retention of Personal Information created as a by-product of the use of the Digital Identity Ecosystem.
214	16	The Governing Body **MUST** clearly define the boundaries of the Digital Identity Ecosystem.
215	17	The Governing Body **MUST** define and implement processes for providing oversight and enforcement of requirements concerning use, disclosure, and retention of Personal Information created as a by-product of the use of the Digital Identity Ecosystem.
216	**ACCU**	**Principle 6 - Accuracy** *Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.*
217	1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the process for a Subject to update inaccurate Personal Information within the Digital Identity Ecosystem is clear and straightforward.
218	2	The Disclosing Organization **MUST** implement policies, procedures, and systems to identify, correct and manage (e.g., updating Subject records) out-dated Personal Information. An organization will only know that the information is out-dated if it asks someone (e.g., the subject for periodic verification), or receives push notifications of updates. Optimal or available options to maintain this information will vary by use case and specific circumstances.
219	3	The Disclosing Organization **MUST NOT** share Personal Information that is known to be invalid, such as an address where the organization has received returned mail.
220	4	When sharing the Personal Information of a Subject with a Requesting Organization, the Disclosing Organization **MUST** provide the Subject with: 1. the ability to review his/her Subject's Personal Information that is to be shared; and 2. instructions or the means to update such Subject's Personal Information.
221	5	When sharing Service Information of a Subject with a Requesting Organization, the Disclosing Organization or Notice and Consent Processor **SHOULD** provide the Subject with: 1. the ability to review his/her Service Information that is to be shared; and 2. instructions or the means to update such Service Information.
222	6	To verify the accuracy of the Personal Information received from the Disclosing Organization, the Requesting Organization **SHOULD** provide the Subject the ability to review the information disclosed. Where the Personal Information obtained from the Digital Identity Ecosystem conflicts with Personal Information that the Requesting Organization holds, the Requesting Organization **MUST** resolve this within its own operation.

223	7	The Notice and Consent Processor **MUST** store an audit trail of notice and consent information, which could include evidence of inaccurate information shared in the past. The integrity of this audit trail must be maintained. The retention period for the audit trail will be determined by the governance framework and applicable legislation and regulation.
224	8	The Governing Body **MUST** define and place rules around how the accuracy of Personal Information can be supported by the Digital Identity Ecosystem. This may include, for example, services that allow (with the Subject's consent) broadcast of updates to subscribed Requesting Organizations.
225	**SAFE**	**Principle 7 - Safeguards** *Personal information must be protected by appropriate security relative to the sensitivity of the information.*
226	1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure security measures to protect Personal Information are in place and communicated to the Subject, and that protections are in place in the event something goes wrong.
227	2	The Disclosing Organization **MUST** develop and implement a security policy to protect Personal Information that specifically includes protections employed in the disclosure of the Subject's Personal Information in the context of the digital identity systems concerned.
228	3	The Disclosing Organization **MUST** implement appropriate security safeguards to protect access to Personal Information, both at rest and in transit.
229	4	The Disclosing Organization **MUST** employ security safeguards appropriate to the sensitivity of Personal Information to the Subject and as well as to the risk of fraud or abuse.
230	5	The Disclosing Organization **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.
231	6	The Requesting Organization **MUST** develop and implement a security policy to protect Personal Information that specifically includes protections employed in the receipt of Personal Information in the context of the digital identity systems concerned.
232	7	The Requesting Organization **MUST** implement appropriate security safeguards to protect access to Personal Information, both at rest and in transit.
233	8	The Requesting Organization **MUST** employ security safeguards appropriate to the sensitivity of Personal Information to the Subject and as well as to the risk of fraud or abuse.
234	9	The Requesting Organization **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.
235	10	The Notice and Consent Processor **MUST** develop and implement a security policy to protect Personal Information that specifically includes protections employed in the Notice and Consent processes.

236	11	The Notice and Consent Processor **MUST** implement appropriate security safeguards.
237	12	The Notice and Consent Processor **MUST** employ security safeguards appropriate to the sensitivity of Personal Information to the Subject and as well as to the risk of fraud or abuse.
238	13	The Notice and Consent Processor **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.
239	14	The Network Provider **MUST** develop and implement a security policy appropriate to the function of the network. This will normally involve ensuring that the Network Provider minimizes its visibility of Personal Information.
240	15	The Network Provider **MUST** implement appropriate security safeguards.
241	16	The Network Provider **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.
242	17	The Governing Body **MUST** implement governance arrangements to include minimum security standards, assessment of participant security arrangements (where appropriate) and placing contractual obligations on participants to meet minimum security standards.
243	**OPEN**	**Principle 8 - Openness** *An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.*
244	1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the Subject is able to readily obtain clear and understandable information concerning the Digital Identity Ecosystem, how the Subject's privacy is protected, where to go for more information and who to contact for help.
245	2	The Disclosing Organization **MUST** provide help and guidance when a Subject makes an access request pertaining to a different part of the Digital Identity Ecosystem that the Disclosing Organization has no visibility of. For example, in a blinded ecosystem the Disclosing Organization may not know which Requesting Organization the Personal Information has been shared with, but it should be able to explain that to the Subject and advise them to contact the Requesting Organization.
246	3	The Disclosing Organization **MUST** provide information to Subjects concerning the Disclosing Organization's role following the Governing Body guidelines.
247	4	The Disclosing Organization **MUST** ensure information concerning the Disclosing Organization's role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se).
248	5	The Requesting Organization **MUST** provide help and guidance when a Subject makes an access request pertaining to a different part of the Digital Identity Ecosystem that the Requesting Organization has no visibility of.

249	6	The Requesting Organization **MUST** provide information to Subjects concerning the Requesting Organization's role following the Governing Body guidelines.
250	7	The Requesting Organization **MUST** ensure information concerning the Requesting Organization's role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se).
251	8	The Notice and Consent Processor **MUST** provide help and guidance when a Subject makes an access request pertaining to a different part of the Digital Identity Ecosystem that the Notice and Consent Processor has no visibility of.
252	9	The Notice and Consent Processor **MUST** provide information to Subjects concerning the Notice and Consent Processor's role following the Governing Body guidelines.
253	10	The Notice and Consent Processor **MUST** ensure information concerning the Notice and Consent Processor's role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se).
254	11	The Network Provider **MUST** provide information to Subjects concerning the Network Provider's role following the Governing Body guidelines.
255	12	The Network Provider **MUST** ensure information concerning the Network Provider's role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se).
256	13	The Governing Body **MUST** ensure that the policies and practices for the management of Personal Information by the Digital Identity Ecosystem are clear, consistent and complete.
257	14	The Governing Body **MUST** work with the ecosystem's participants to ensure all information is presented in a consistent manner to avoid conflicting or confusing messages.
258	15	The Governing Body **MUST** provide guidelines to all participants on compliance with the requirements statements noted above in this section, and review conformance by the participants to ensure it follows the guidelines.
259	16	The Governing Body **MUST** ensure that there are processes in place to respond to a Subject's request for information.
260	**INDI**	**Principle 9 - Individual Access** *Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and 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.*

261	1	Participants in the Digital Identity Ecosystems will often provide inbuilt features that automatically provide the Subject with information concerning the existence, use, and disclosure of their Personal Information within the Digital Identity Ecosystem. Where such features exist, Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the principle of individual access (as described in PIPEDA) is met. When participants in the Digital Identity Ecosystem do not provide inbuilt features providing the Subject with information concerning the existence, use, and disclosure of their Personal Information, then the process for obtaining such information **MUST** be clear, straightforward and in line with PIPEDA.
262	2	The Disclosing Organization **MUST** provide clear means for the Subject to obtain information concerning the existence, use and disclosure of their Personal Information within the context of the Digital Identity Ecosystem.
263	3	The Requesting Organization **MUST** provide clear means for the Subject to obtain information concerning the existence and use of their Personal Information received via the Digital Identity Ecosystem.
264	4	When the Subject notifies the Requesting Organization that the Personal Information it holds or uses is inaccurate or incomplete, the Requesting Organization **MUST** have appropriate processes in place to correct or amend the Personal Information. This may include: • re-requesting the information from the Disclosing Organization(s) via the Digital Identity Ecosystem; and • independently working with the Subject to determine the correct Personal Information.
265	5	If the Requesting Organization determines that the Personal Information it receives from the Digital Identity Ecosystem is inaccurate or incomplete, processes **MAY** exist to notify the relevant Disclosing Organization of the problem.
266	6	The Notice and Consent Processor **MUST** provide clear means for the Subject to obtain information concerning the existence, use, and disclosure of their Personal Information within the Notice and Consent Processor. Because the Notice and Consent Processor exists to facilitate the sharing of Personal Information but then does not subsequently use the Personal Information, the "individual access" is likely to be limited to viewing the audit trail of Notice and Consent activities relating to the Subject.
267	7	The Network Provider **SHOULD NOT** have access to Personal Information (other than potentially anonymous identifiers that the Network cannot link back to Subjects). If the Network Provider does have access to Personal Information, then the Network Provider **MUST** comply with the PIDEDA "Information Access" principle.
268	8	The Governing Body governance arrangements **MUST** ensure that "Information Access" processes are provided appropriate to the Digital Identity Ecosystem.

269	**CHAL**	**Principle 10 - Challenging Compliance** *An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.*
270	1	The name or title of the person responsible for compliance in the Disclosing Organization, Requesting Organization and Notice and Consent Processor, and means to engage in recourse against them, **MUST** be made simple and available.
271	2	The Disclosing Organization **MUST** have a compliance management program that: • clearly and simply differentiates involvement in the Digital Identity Ecosystem from the organization's other activities; and • assists the Subject in obtaining the support required, even if the complaint needs to be directed to another participant in the Digital Identity Ecosystem.
272	3	The Requesting Organization **MUST** have a compliance management program that: • clearly and simply differentiates involvement in the Digital Identity Ecosystem from the organization's other activities; and • assists the Subject in obtaining the support required, even if the complaint needs to be directed to another participant in the Digital Identity Ecosystem.
273	4	The Network Provider **MUST** have a compliance management program that: • clearly and simply differentiates involvement in the Digital Identity Ecosystem from the organization's other activities; and • assists the Subject in obtaining the support required, even if the complaint needs to be directed to another participant in the Digital Identity Ecosystem.
274	5	The Governing Body **MUST** ensure that any organization operating within the Digital Identity Ecosystem follows Principle 10.
275	6	The Governing Body **MUST** put in place processes to triage and direct complaints in order that the Subject is provided with the necessary support from the correct participant, as efficiently and clearly as possible.
276	7	The Governing Body **MUST** include procedures on how to notify and respond to complainants in a timely manner as well as record decisions and actions to ensure consistency with the Privacy Conformance Profile and to protect the participants of the Digital Identity Ecosystem.