PCTF Privacy Conformance Profile

Document Status: Final Recommendation V1.0

In accordance with the DIACC Operating Procedures, a Final Recommendation is a deliverable that represents the findings of a DIACC Expert Committee that have been approved by an Expert Committee and have been ratified by a DIACC Sustaining Member Ballot.

This document was developed by DIACC's Trust Framework Expert Committee with input from the public gathered and processed through an open peer review process. It is anticipated that the contents of this document will be reviewed and updated on a regular basis to address feedback related to operational implementation, advancements in technology, and changing legislation, regulations, and policy. Notification regarding changes to this document will be shared through electronic communications including email and social media. Notification will also be recorded on the Pan-Canadian Trust Framework Work Programme. Changes to this document that may affect certification and Trustmark status will be defined in the Pan-Canadian Trust Framework Assessment component.

Table of Contents

1 Introduction to the PCTF Privacy Conformance Profile

This document specifies the Conformance Criteria of the PCTF Privacy Component, a component of the Pan-Canadian Trust Framework (PCTF). For a general introduction to the PCTF, including contextual information and the PCTF goals and objectives, please see the PCTF Model Overview.

The Conformance Criteria for the Privacy Component specify how the Principles in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), defined in Schedule 1 of the legislation, are relevant/apply to the handling of digital identity data. PIPEDA applies to organizations handling personal information in the course of commercial activities.

Notes

- These conformance criteria do not replace existing regulation; organizations are expected to comply with relevant privacy legislation, policy and regulations in their jurisdiction.
- In the Privacy conformance criteria, the phrase "notice and consent" is to be interpreted as "notice, or notice with consent" recognizing there are use cases where notice is required but explicit consent is not required/sought.

1.1 Conformance Criteria Keywords

The following keywords are used in the conformance criteria to indicate their precedence and/or general rigidity, and are to be interpreted as:

- **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 choosing to not adhere to the conformance criteria or choosing a different option as specified by the conformance criteria.
- **SHOULD NOT** means that a valid exception 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.

Note

- The above keywords appear in **bold typeface** and ALL CAPS throughout this conformance profile.

2 Privacy Component Conformance Criteria

The conformance criteria listed below are organized and intended to align with the Principles in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), defined in Schedule 1 of the legislation. The descriptions of the principles included below are taken from the PIPEDA's fair information principles on the Office of the Privacy Commissioner. For ease of reference, a specific conformance criterion 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 Facilitator and the Governing Body **MUST** have a privacy management program in place to ensure compliance with applicable law including the implementation of privacy policies, practices, controls and assessment tools.
2	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** have a designated privacy official 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).
3	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators 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.
4	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** periodically audit or perform a review of their personal information management practices (including its notice and consent management practices), to a maximum of 3 years between audits or reviews, to ensure that Personal Information is being handled in the way described by its privacy policy.
5	The Governing Body **MUST** ensure organizations operating within the Digital Identity Ecosystem comply with the conformance criteria listed for Principles 1-10.

6	As part of their privacy management programs, Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** have processes to manage Personal Information breaches or breaches of confidentiality, which includes assessing damage or harm, reporting, containment, remediation, notification, and prevention steps.
7	The Governing Body **MUST** clearly define and manage the boundaries of the Digital Identity Ecosystem.
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.*
1	Disclosing Organizations, Requesting Organizations, Network Facilitators, and Notice and Consent Processors **MUST** ensure the User has a clear idea of who (e.g. designation, contact information) is responsible for privacy in their respective organizations.
2	Disclosing Organizations, Requesting Organizations, Network Facilitators, and Notice and Consent Processors **MUST** make the name or title of the person who is responsible for privacy in their respective organizations readily available to the User and provide them with the means to contact that person.
3	The Disclosing Organization **MUST** have a privacy management program that includes: • if applicable, restrictions based on the type of organizations with whom the Subject-Specific Personal Information will be shared or restrictions based on the purpose for collecting that information. For example, there may be restrictions 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-Specific Personal Information; • if applicable, restrictions on the process of sharing the Subject-Specific Personal Information; • processes to be followed when the Subject-Specific Personal Information is shared; • processes to be followed when the Subject-Specific Personal Information previously shared is updated, deleted or expired; • clear guidance for Users on the sharing of the Subject-Specific Personal Information to help them know which party they should contact depending on the nature of their inquiry; • data protection controls; and • privacy impact assessment that explicitly covers the disclosure of the Subject-Specific Personal Information through the Digital Identity Ecosystem.

4	Disclosing Organizations, Requesting Organizations, and Notice and Consent Processors **MUST** ensure that the responsibilities of their designated official include the authority to intervene on privacy issues specifically relating to the organization's role as a Disclosing Organization, Requesting Organization, or Notice and Consent Processor. This may be delegated but the original processor remains accountable. This will ensure a holistic and consistent approach to the protection of the Subject's privacy.
5	The Requesting Organization **MUST** have a privacy management program that includes: • if applicable, restrictions based on the type of organizations from whom the Subject-Specific Personal Information will be obtained or restrictions based on the purpose for collecting that information. For example, there may be restrictions based on sector, regulatory environment (e.g., health, financial services); • if applicable, processes to be followed when the Disclosing Organization defines specific requirements to the Requesting Organization regarding the handling of Subject-Specific Personal Information; • if applicable, restrictions on the process of obtaining the Subject-Specific Personal Information; • processes to be followed when the Subject-Specific Personal Information is obtained via the digital identity system; • processes to be followed when the Subject-Specific 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 their inquiry; • data protection controls; and • privacy impact assessment that explicitly covers the use of the Subject-Specific Personal Information obtained through the Digital Identity Ecosystem. Suggest limiting the Notice & Consent Processor’s responsibility to changes that affect the Subject’s stored consent directive state. Suggest change as follows: “previously shared is updated, deleted or expired. The Notice & Consent Processor must have processes in place to manage changes affecting the Subject’s stored consent directive, specifically the consent directive’s state.”

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, the Notice and Consent Processor should never be in possession of or store the Subject-Specific Personal Information; • if applicable, processes to be followed when the Disclosing Organization defines specific requirements to the Notice & Consent Processor regarding the handling of Subject-Specific Personal Information; • processes to be followed when facilitating the sharing of the Subject-Specific Personal Information; • processes to be followed for the management of consent by the Subject • processes to be followed when the Subject-Specific Personal Information previously shared is updated, deleted or expired; • clear guidance for Subjects on the sharing of the Subject-Specific Personal Information to help them know which party they should contact depending on the nature of their inquiry; • data protection controls; and • privacy impact assessment that explicitly covers the facilitation role, focusing on minimizing (or even eliminating) access to or visibility of the Subject-Specific Personal Information or Service-Specific Information.
7	The Network Facilitator **MUST** have a privacy management program that includes: • restrictions on use of Personal Information where the Network Facilitator is just a facilitator, for example, potentially the Network Facilitator must never be in possession of, or store, the Subject-Specific Personal Information; • if applicable, processes to be followed when facilitating the sharing of the Subject-Specific Personal Information; • processes to be followed when the Subject-Specific Personal Information previously shared is updated, deleted or expired; • clear guidance for Subjects on the sharing of the Subject-Specific Personal Information to help them know which party they should contact depending on the nature of their inquiry; • data protection controls; and privacy impact assessment that explicitly covers the facilitation role, focusing on minimizing (or even eliminating) access to or visibility of the Subject-Specific Personal Information or Service-Specific Information.

8	The Governing Body **MUST**: • ensure accountability of the organizations operating with the Digital Identity Ecosystem; • If applicable, ensure that specific requirements defined by an organization on a Subject-Specific Personal Information are complied with by relevant Digital Identity Ecosystem participants; • include rules concerning standards and interoperability that ensure all parties involved in the sharing of the Subject-Specific Personal Information treat the Subject and the Subject-Specific 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 relevant privacy regulators and individuals; and • facilitate monitoring of operational risks (e.g., fraud, information security) across the Digital Identity Ecosystem.
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.*
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.
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.
3	The Requesting Organization **MUST** clearly identify the purpose for collecting Subject-Specific Personal Information through the Notice and Consent Processor.
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.
5	The Requesting Organization **MUST** periodically, to a maximum of 3 years between reviews, perform an internal review of their Personal Information collection and use requirements, and update future requests accordingly.
6	The Requesting Organization **MUST** ensure that the reasons for the collection and use of Subject-Specific Personal Information are clear, unambiguous, and not overly broad.
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.

8	The Governing Body **MUST** 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.
9	The Governing Body **MUST** ensure organizations operating within the Digital Identity Ecosystem comply with the conformance criteria listed for Principles 2, and evidence of the Requesting Organizations compliance can be provided to Disclosing Organizations.
10	The Governing Body **MUST** include procedures to investigate and address deviations from Principle 2.
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.*
1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the notice and knowledge required for the consent request is clear, understandable and meaningful to the User.
2	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** ensure the consent process balances sufficient information to the User against information overload. In all cases, a straightforward means **SHOULD** be provided for the User to get additional information, as may be required.
3	The Disclosing Organization **MUST** ensure the Notice and Consent Processor performs its function of providing notice and recording/managing consent appropriately prior to disclosing the Subject-Specific Personal Information.
4	The Disclosing Organization **MUST** ensure that evidence of the notice and consent is obtained by the Notice and Consent Processor and then stored appropriately.
5	The Disclosing Organization **MUST** confirm notice and consent is not expired or revoked at the time of sharing a Subject-Specific Personal Information. In the event the consent is not expired or revoked, the Requesting Organization **MUST** be provided with a response that indicates the consent is valid.
6	The Disclosing Organization **MUST** ensure the User has access to the information required to understand the nature, purpose, and risks associated with the use or disclosure, of their Subject-Specific Personal Information, within the Digital Identity Ecosystem. For example, via the Privacy notice statement. See also NOTI-5 in the PCTF Notice and Consent component.
7	The Requesting Organization, as the originator of the request for consent, **MUST** be responsible for defining the purpose of processing the requested Subject-Specific Personal Information in the content of the notice. See also NOTI-5 in the PCTF Notice and Consent component.

8	The Requesting Organization as the originator of the request for consent, **MUST** be primarily responsible for defining the nature of the sharing request in the content of the notice. Note: Nature of sharing refers to whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure.
9	The Requesting Organization **MUST** ensure that the request follows a principle of minimal disclosure.
10	The Requesting Organization **MUST** ensure the Notice and Consent Processor performs its function of providing notice and recording/managing consent appropriately prior to receiving Subject-Specific Personal Information.
11	The Requesting Organization **MUST** ensure that a record of the notice and consent is obtained by the Notice and Consent Processor and then stored appropriately.
12	When the Requesting Organization is made aware that consent is no longer valid, the Requesting Organization **MUST** cease further collection of Subject-Specific Personal Information based on this invalidated consent.
13	The Notice and Consent Processor **MUST** be responsible for providing notice to the User within the Digital Identity Ecosystem.
14	The Notice and Consent Processor **MUST** ensure its notice clearly reflects the nature of sharing within the Digital Identity Ecosystem. Note: Nature of sharing refers to whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure.
15	The Notice and Consent Processor **MUST** ensure, or receive confirmation, the User is authenticated prior to displaying any Subject-Specific Personal Information within a notice to the User by validating the identity of the User.
16	The Disclosing Organization **MUST** define the sensitivity of the Personal Information being shared and implement their rules (e.g., masking policies) for the display of sensitive information within the notice.
17	The Notice and Consent Processor **MUST** be able to display Personal Information in the notice in accordance with any rules (e.g., masking policies) stipulated by the Disclosing Organization.
18	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).
19	The Notice and Consent Processor **MUST** record the consent and provide the User with means to review and manage any consents given.
20	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.

21	The Notice and Consent Processor **MUST** have processes in place to support the revocation of consent. For example, an action to revoke consent could originate from the Subject or be in response to the detection of fraudulent activity by any one of the digital identity processing organizations.
22	The Network Facilitator **MAY** be involved in determining or discovering which Disclosing Organizations are potential sources of the requested Personal Information. Note: As an alternative, for example, Requesting Organizations may directly specify the required source.
23	The Network Facilitator **MUST NOT** have visibility to unprotected Personal Information shared through the Digital Identity Ecosystem. Specifically, this includes any Personal Information presented in the notice and consent process, as well as transmission of Personal Information through the network.
24	The Governing Body **MUST** provide guidelines on the formulation of notices and collection of consent, to provide a consistent and optimized user experience across the Digital Identity Ecosystem.
25	The Governing Body **MUST** include procedures to investigate and manage deviations from Principle 3, including assessing the risk to Subjects and reporting breaches to relevant privacy regulators and Subjects.
26	The Governing body **MUST** include provisions which ensure that revocation of consent by a User is promptly effective across the entire Digital Identity Ecosystem.
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.*
1	The Disclosing Organization **MUST** have confidence that the Requesting Organization has good and sufficient reason for collecting the requested Personal Information.
2	The Requesting Organization **MUST** clearly delineate Personal Information collection activities via the Digital Identity Ecosystem from other activities of the Requesting Organization.
3	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 Users to access services or prove entitlement.
4	The Requesting Organization **MUST** publicly document, or make available, the kind and purpose of Personal Information collected.
5	The Requesting Organization **MUST** ensure that it educate applicable employees on the kind and purpose of Personal Information collected in order to accurately respond to any 3rd party inquiries.

6	The Requesting Organization **MUST** be clear, unambiguous, and transparent about the reason for collecting Personal Information in all forms of communication.
7	The Notice and Consent Processor **MUST** ensure that Personal Information required to perform the notice and consent function is limited to only that which is required to perform the function.
8	The Network Facilitator **MUST** facilitate the sharing of Personal Information.
9	The Governing Body **MUST** have confidence that the Requesting Organization has good and sufficient reason for collecting the requested Personal Information.
10	The Governing Body **MUST** define rules and guidelines on appropriate ways to limit collection of Personal Information within and by the Digital Identity Ecosystem participants.
11	The Governing Body **MUST** include procedures to investigate and manage deviations from Principle 4, including assessing the risk to Subjects and reporting breaches to relevant privacy regulators and Subjects.
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.*
1	The Disclosing Organization **MUST** have internal policies and other documentation for limiting use, disclosure, and retention of Subject-Specific Personal Information.
2	The Disclosing Organization **MUST** document uses of Subject-Specific Personal Information for the purpose of disclosure within the Digital Identity Ecosystem.
3	If there is a defined minimum and maximum data retention policy specified for the Digital Identity Ecosystem, the Disclosing Organization **MUST** comply with that policy with respect to the Subject-Specific Personal Information in connection with the Digital Identity Ecosystem. Note: Subject to regulatory restrictions.
4	The Disclosing Organization **MUST** limit disclosure of the Subject-Specific Personal Information to only that required for the specific and intended purpose in alignment with Subject's consent, unless otherwise permitted or required by law.
5	The Disclosing Organization **MUST** limit disclosure of the Subject-Specific Personal Information to only that which the Disclosing Organization has confidence in the accuracy and currency of.
6	The Requesting Organization **MUST** document uses of Subject-Specific Personal Information received via the Digital Identity Ecosystem.

7	Requesting Organizations and Notice and Consent Processors **MUST** institute maximum and minimum valid retention periods of the Subject-Specific Personal Information received via the Digital Identity Ecosystem.
8	The Requesting Organization **MUST NOT** use or retain, without obtaining proper consent, the Subject-Specific 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.
9	The Notice and Consent Processor **MUST** have internal policies and other documentation for limiting use, disclosure, and retention of Personal Information.
10	The Notice and Consent Processor **MUST** document the use of the Subject-Specific Personal Information for the 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. However, this is dependent on both the implementation and the requirements to present the Subject-Specific Personal Information itself as part of the consent process.
11	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.
12	The Network Facilitator **MUST** facilitate the establishment of systems for the sharing of Personal Information.
13	The Certifying Authority **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.
14	The Certifying Authority **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.
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.*
1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure the process for a User to update inaccurate Personal Information within the Digital Identity Ecosystem exists, and clearly lays out the responsibilities of each party within the Digital Identity Ecosystem including the User's own responsibility.

2	The Disclosing Organization **MUST** implement policies, procedures, and systems to identify, correct and manage (e.g., updating Subject records) outdated Personal Information. An organization will only know that the information is outdated 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. Please refer to the Verified Person Profile, especially the ID Maintenance section, for related Conformance Criteria.
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.
4	When sharing Subject-Specific Personal Information with a Requesting Organization, the Disclosing Organization **MUST** provide the User with: 1. the ability to review a description or summary of the Subject-Specific Personal Information that is to be shared; and 2. instructions or the means to update such Subject-Specific Personal Information.
5	When sharing Service-Specific Information of a Subject with a Requesting Organization, the Disclosing Organization or Notice and Consent Processor **MAY** provide the User with: 1. the ability to review a description or summary of his/her Service-Specific Information that is to be shared; and 2. instructions or the means to update such Service-Specific Information.
6	To verify the accuracy of the Personal Information received from the Disclosing Organization, the Requesting Organization **SHOULD** provide the User the ability to review a summary or description of the information disclosed.
7	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.
8	The Notice and Consent Processor **MUST** store an audit trail of notice and consent information. 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.
9	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.
SAFE	**Principle 7 - Safeguards** *Personal information must be protected by appropriate security relative to the sensitivity of the information.*

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 User (as appropriate), and that protections are in place in the event something goes wrong.
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-Specific Personal Information in the context of the digital identity systems concerned.
3	The Disclosing Organization **MUST** implement appropriate security safeguards, in accordance with the risks of harm identified in risk assessment (threat risk assessment and/or privacy impact assessment as appropriate), to protect access to Personal Information, both at rest and in transit.
4	The Disclosing Organization **MUST** employ security safeguards, in accordance with the risks of harm identified in risk assessment (threat risk assessment and/or privacy impact assessment as appropriate), appropriate to the sensitivity of Personal Information to the Subject and as well as to the risk of fraud or abuse.
5	The Disclosing Organization **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.
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.
7	The Requesting Organization **MUST** implement appropriate security safeguards to protect access to Personal Information, both at rest and in transit.
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.
9	The Requesting Organization **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.
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.
11	The Notice and Consent Processor **MUST** implement appropriate security safeguards.
12	The Notice and Consent Processor **MUST** employ security safeguards appropriate to the sensitivity of any Personal Information presented to the Subject in the privacy notice as well as to the risk of fraud or abuse.
13	The Notice and Consent Processor **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.

14	The Network Facilitator **MUST** develop and implement a security policy appropriate to the function of the network. This will normally involve ensuring that the Network Facilitator minimizes its visibility of Personal Information.
15	The Network Facilitator **MUST** implement appropriate security safeguards.
16	The Network Facilitator **MUST** conduct a regular review and update of security measures relating to the Digital Identity Ecosystem.
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.
18	Digital Identity Ecosystem Participants **MUST** perform a risk assessment (threat risk assessment and/or privacy impact assessment as appropriate) in order to ascertain the risks associated with their processing of Personal Information.
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.*
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.
2	Disclosing Organizations, Requesting Organizations, and Notice and Consent Processors **MUST** provide help and guidance when a User makes an access request pertaining to a different part of the Digital Identity Ecosystem. This may involve having the User identify the Requesting Organization through activity history, a consent receipt, and/or engaging the Network Facilitator or Governing Body to support identification of the relevant participant.
3	The Disclosing Organization **MUST** provide information to Users concerning the Disclosing Organization's role following the Governing Body guidelines.
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).
5	The Requesting Organization **MUST** provide information to Users concerning the Requesting Organization's role following the Governing Body guidelines.
6	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).

7	The Notice and Consent Processor **MUST** provide information to Users concerning the Notice and Consent Processor's role following the Governing Body guidelines.
8	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).
9	The Network Facilitator **MUST** provide information to Users concerning the Network Facilitator's role following the Governing Body guidelines.
10	The Network Facilitator **MUST** ensure information concerning the Network Facilitator'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).
11	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.
12	The Governing Body **MUST** work with the ecosystem's participants to ensure the privacy policy and practices information required by Openness 8 criteria is presented in a consistent manner to avoid conflicting or confusing messages.
13	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 they follow the guidelines.
14	The Governing Body **MUST** ensure that there are processes in place to respond to a User's request for information.
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.*
1	Participants in the Digital Identity Ecosystems will often provide inbuilt features that automatically provide the User 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 User 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 or other relevant legislation.

2	The Disclosing Organization **MUST** provide clear means for the User to obtain information concerning the existence, use and disclosure of their Personal Information as it pertains to handling of the information within the context of the Digital Identity Ecosystem.
3	The Requesting Organization **MUST** provide clear means for the User to obtain information concerning the existence and use of their Personal Information received via the Digital Identity Ecosystem.
4	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.
5	The Notice and Consent Processor **MUST** provide clear means for the User 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.
6	The Network Facilitator **SHOULD NOT** have access to Personal Information (other than potentially anonymous identifiers that the Network cannot link back to Subjects). If the Network Facilitator does have access to Personal Information, then the Network Facilitator **MUST** comply with the PIPEDA "Individual Access" principle.
7	The Governing Body governance arrangements **MUST** ensure that "Individual Access" processes and guidelines are provided and appropriate to the information exchanged through the Digital Identity Ecosystem.
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.*
1	The name or title, and contact information, 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.

2	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, and Network Facilitators each **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 User in obtaining the support required, even if the complaint needs to be directed to another participant in the Digital Identity Ecosystem.
3	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.
4	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.

3 Revision History

Version Number	Date of Issue	Author(s)	Description
0.01	2018-08-08	Privacy Design Team	Initial working draft
0.02	2018-09-28	Privacy Design Team	Added 10 Principles
0.03	2018-11-09	Privacy Design Team	Incorporated feedback from Nov. 8 Deep Dive meeting
0.04	2018-11-22	Privacy Design Team	Grammatical cleanup and updated terms for roles: • "Network" to "Network Provider' • "Eco-System" to "Governing Body"
0.05	2018-12-24	Privacy Design Team	Incorporated feedback from Dec. 20 Deep Dive meeting
0.06	2019-01-04	Privacy Design Team	Incorporated feedback from Jan. 3 meeting
0.07	2019-01-17	Privacy Design Team	Incorporated feedback from Jan. 17 meeting
0.08	2019-02-14	Privacy Design Team	Incorporated feedback from Feb. 14 meeting
0.09	2019-05-09	Privacy Design Team	Incorporated feedback from Apr. 17 meeting
0.10	2019-05-09	PCTF Editing Team	Updated conformance criteria numbering
0.11	2019-06-26	PCTF Editing Team	Incorporated comments from discussion draft open review
0.12	2019-07-05	PCTF Editing Team	Updates based on July 4th Privacy Design meeting to resolve remaining comments
0.13	2019-11-22	PCTF Editing Team	Applied standard outline for PCTF Conformance Profile, which consolidates conceptual information in the Overview.
0.14	2019-12-05	PCTF Editing Team	Updates base on comment resolution from open review.
0.15	2020-01-02	PCTF Editing Team	Updated based on suggested editorial changes from open review.

0.16	2020-01-07	Privacy Design Team	Updated based on in-person Privacy Design Team review of comments.
0.17	2020-02-12	PCTF Editing Team	Updated based on several consultation sessions with TFEC expert team to review received TFEC comments
1.0	2020-02-24	PCTF Editing Team	Approve as Draft Recommendation V1.0
1.1	2020-05-20	PCTF Editing Team	Changed "Governing Body" to "Certifying Authority" to match Assessment component.
1.2	2020-05-28	PCTF Editing Team	Updated draft as per comments and resolutions from open review.
1.0	2020-07-02	PCTF Editing Team	Final Recommendation V1.0