PCTF Privacy

Document Status: Final Recommendation V1.2

In accordance with the DIACC Operating Procedures, Final Recommendations are 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.

Table of Contents

1. Introduction to the PCTF Privacy Component

Content herein concerns itself with the domain specific topic for this Pan-Canadian Trust Framework (PCTF) component. The overview section provides information related to and necessary for consistent interpretation of the included conformance criteria. For a general introduction to the PCTF, please see the PCTF Overview that describes the background, purpose, scope, principles, and objectives of the framework.

1.1. Purpose and Anticipated benefits

Privacy is a fundamental requirement of digital identity interactions. As such, all participants in the Pan-Canadian Trust Framework (PCTF) have a responsibility to follow privacy-respecting practices. Privacy-respecting practices rely on the principle that individuals know and understand the details and potential benefits, risk of harm and consequences associated with managing their personal information, and can take action based on that information.

The Privacy Component of the PCTF is concerned with the handling of personal data for digital identity purposes. The objective of the Privacy Component is to ensure the ongoing integrity of the privacy processes, policies and controls of organizations in a Digital Identity Ecosystem by means of standardized conformance criteria used for assessment and certification against the Pan-Canadian Trust Framework (PCTF). The Conformance Criteria for the Privacy Component specify tests that can be used to assess that an organization performing the role of Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Providers, or the Governing Body. The Conformance Criteria are designed to demonstrate that participants are handling digital identity information in alignment with the ten Principles defined in Schedule 1 of the Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) legislation. PIPEDA applies to organizations handling personal information in the course of commercial activities.

Note: The current set of conformance criteria are organized by the ten Principles for the Protection of Personal Information in Schedule 1 of PIPEDA[1]; however, they are intended to be broadly applied across private and public sector organizations. Future versions of this component may incorporate additional conformance criteria after review of other privacy guidance (e.g., Privacy by Design, PIPEDA modernization) and regulatory frameworks (e.g., federal and provincial privacy acts).

These conformance criteria do not replace existing regulations; organizations are expected to comply with relevant privacy legislation, policy and regulations in their jurisdiction.

Figure 1 provides a conceptual overview and logical organization of the Privacy Component.

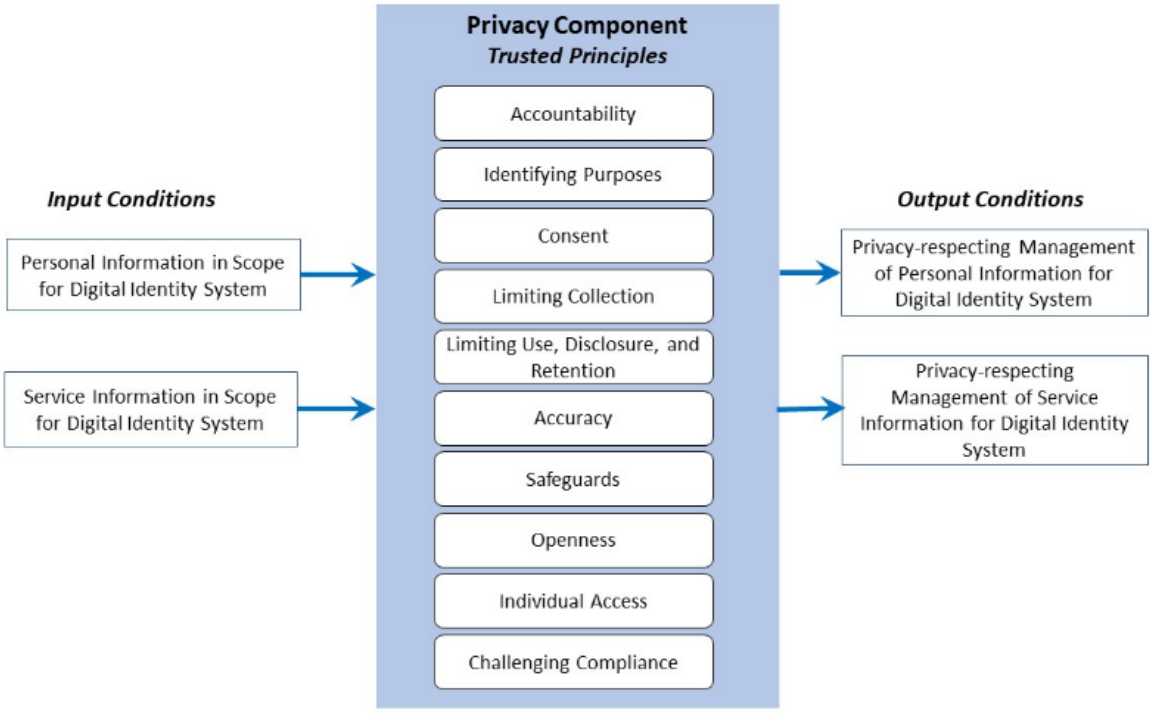

Figure 1. Privacy Component

The Privacy Component consists of elements that indicate the following:

- **Trusted Principles** – the set of principles that organizations (e.g., Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators) are expected to adhere to when handling subject-specific and service-specific personal information in a digital identity system. Each trusted principle is assessed using a set of conformance criteria associated with that principle.
- **Inputs** – input into trusted principles, for example, personal information requiring privacy management to proceed.
- **Outputs** – output resulting from trusted principles being applied, for example, privacy policies and controls applied to personal information.

1.2. Scope

Figure 2 illustrates the scope of the privacy component, which includes the functions performed by the Disclosing Organization, Requesting Organization, Notice and Consent Processor, as well as the Network Facilitator and Governing Body roles as described in the Roles section.

In the PCTF context, Personal Information (as defined in the Terms and Definitions section) will normally only be accessed by those performing roles that process digital identity information within the Digital Identity Ecosystem, and who will restrict access for those purposes. Participants that perform roles in the Digital Identity Ecosystem to enable, control and implement rules to facilitate the sharing of personal information, ideally (e.g., unless required by law)) should not be able to see, read, change, or be exposed to the information. The Notice and Consent Processor, which performs control functions, could be exposed to some personal information in (depending on how the Notice and Consent Processor is manifested), but this should be minimized (as per conformance criteria for limiting collection LIMC-9).

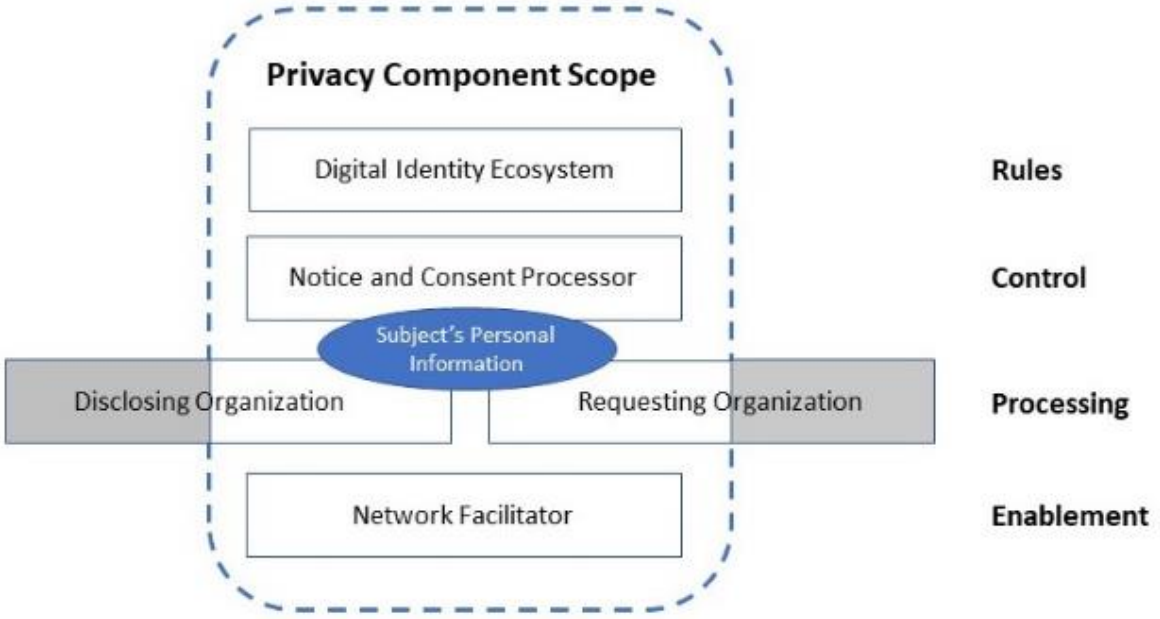

Figure 2. Privacy Component Scope and Roles

1.2.1. In-Scope

- Within the context of the PCTF, privacy requirements applicable to the roles within the Digital Identity Ecosystem. For an overview description of the PCTF model and its components, please refer to the PCTF Model Overview
- Requirements for the handling of Subject-Specific Personal Information and Service-Specific information associated with digital identity
- Privacy related policy and processes as they apply to delivery of assured digital identity

1.2.2. Out-of-Scope

- Fraud monitoring: The Privacy component does include conformance criteria that address breaches of privacy and fraud reporting for the roles specific to the

Privacy component. Requirements for more general fraud monitoring, reporting, and actions to be taken within the Digital Identity Ecosystem warrant further consideration and development within the PCTF context. For reference, please consult the following criteria:
    - Baseline - BASE 6
    - For Governing Body - ACCO 2
    - For Notice and Consent Processor - CONS-21
- Specific related requirements addressed in other PCTF profiles (e.g. Delegated authority, Privacy and Security section of the Verified Organization Conformance Profile, requirement SOUR-01 in the Verified Person Conformance Profile)
- Baseline conformance criteria (See BASE in the Privacy Conformance Profile) do not address use cases where the Subject acts as the Disclosing Organization.
- Criteria variance dependent on LoA levels: The DIACC is currently working on the specifics of the LoA framework to be applied. While the work is mature enough to be reflected in some of the Profiles, it was felt that further detail was required in order to define any variances in criteria for the Privacy Component.

1.3. 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 Identity Ecosystem.

Figure 3 is an illustration of the components of the Pan-Canadian Trust Framework. The Privacy Component encompasses all sub-components (i.e., Privacy related concerns are applicable to elements of all PCTF Profiles).

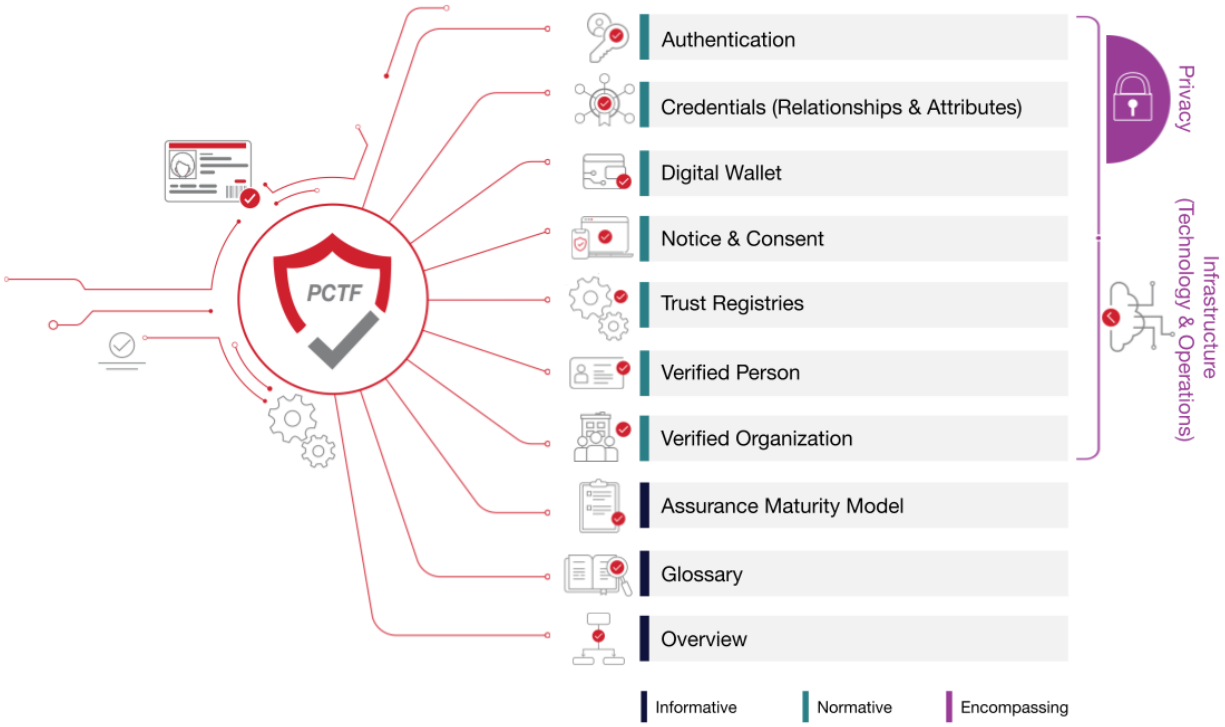

Figure 3. Components of the Pan-Canadian Trust Framework

PCTF conformance criteria do not replace or supersede existing regulations; organizations and individuals are expected to comply with relevant legislation, policy and regulations in their jurisdiction.

2. Privacy Component Conventions

This section describes and defines key terms and concepts used in the PCTF Privacy Component. This information is provided to ensure consistent use and interpretation of terms appearing in this overview and the PCTF Privacy Conformance Profile.

2.1. Terms and Definitions

The Privacy component references the terms and definitions listed in the PCTF Glossary and specifically uses the following terms and definitions:

Subject

A Person, Organization, or Machine that holds or is in the process of obtaining a digital representation in the digital identity ecosystem system regulated by the PCTF, and that can be subject to legislation, policy and regulations within a context. (Note: Delegated Authority is not addressed in this document).

User

A Person who is either the Subject or authorized to represent the Subject and intentionally accessing a digital service or digital program.

Notice

A statement that is formulated to describe the collection, use and disclosure of Personal Information and is presented to a User. May also be referred to as: consent form, or notice statement.

Consent

Permission, given from a User authorized to do so, to share Identity and/or Personal Information about a Subject as per the terms defined in a Notice. In the context of the PCTF, consent is equated to "Meaningful Consent" as described by the Office of the Privacy Commissioner of Canada and PIPEDA. May also be referred to as: consent decision.

Unless explicitly stated, consent in the Privacy component refers to express, or explicit, consent for sharing Personal Information, where the Subject must perform an action to provide consent. Implied consent, if applicable, will be identified as such in the criteria.

Personal Information

In general, Personal Information is defined as "Under PIPEDA, personal information includes any factual or subjective information, recorded or not, about an identifiable individual." For the purpose of this document, we define two types of Personal Information:

- **Service-Specific Information –** information collected or generated by the participants (Disclosing Organization, Requesting Organization, Notice and Consent Processor(s), or Network Facilitator) for purposes of operating and maintaining the service (e.g., service specific pseudonymous identifiers, transaction records, proofs of transactions including consent). In some cases, service-specific information may be shared, with subject's consent.
- **Subject-Specific Personal Information –** factual or subjective information about an identifiable Subject that is shared from a Disclosing Organization to a Requesting Organization (e.g., name, email address, phone number, mailing address, date of birth, account information).

Digital Identity Ecosystem

An interconnected system for the exchange and verification of digital identity information, involving public and private sector organizations (e.g., government,

commercial, non-profit, and other entities) who participate in, and comply with a common Trust Framework for the management and use of digital identities, and the Subjects of those digital identities. In the context of the Privacy component, the Digital Identity Ecosystem refers to a Canadian Digital Identity Ecosystem compliant with the PCTF. Participants in a Digital Identity Ecosystem may include Requesting Organization, Disclosing Organization, Notice and Consent Processor, Network Facilitator, and Governing Body as identified in the Scope section of this document.

3. Roles

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

- **Disclosing Organization –** A Role that an Organization or Person performs to hold Subject-Specific Personal Information, that the User consents to disclose to a Requesting Organization or that the Disclosing Organization can lawfully disclose under relevant legislation. In a digital identity context, this will often be an identity or attribute provider.
- **Governing Body –** A Role that a Participant performs to make sure that the standards, processes, and the associated requirements of the Digital Identity Ecosystem are implemented, which include conformance with government legislation, regulations and policy. They also enforce compliance by Digital Identity Ecosystem participants to agreed safeguards, guidance, best practices, rules and commercial arrangements.
- **Notice and Consent Processor –** A Role that a Participant performs to provide the notice to the User of the request for Personal Information (from the Requesting Organization), to obtain and record the consent and provides the User with the means to manage the consent going forward, including the withdrawal of consent.
- **Network Facilitator –** A Role that a Participant performs to connect 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). For example, a blockchain provider, or Software as a Service provider (SaaS) that facilitates the network.
- **Requesting Organization –** A Role that an Organization or Person performs to receive Personal Information that the User consents to disclose. In a digital identity context, this will often be a service provider or relying party.

These roles help to isolate the different functions and responsibilities with respect to privacy across the end-to-end processes for managing digital identities. 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 User, 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.

4. Privacy Component Key Concepts

4.1. Personal Information

Privacy-respecting practices rely on the principle that individuals know and understand the details and potential benefits and consequences associated with managing their personal information, and can take action based on that information.

Personal information, as defined for the purposes of this Profile, includes Subject-Specific Personal Information and Service-Specific Information. This encompasses information that the user consents to disclose (e.g., name, email address, phone number, mailing address, date of birth, account information, etc.) as well as information required to operate and maintain the service (e.g., service specific pseudonymous identifiers, transaction records).

4.2. Changes of Personal Information at Source (a Disclosing Organization)

In the event of a change (including corrections) to Subject-Specific Personal Information, the Disclosing Organization is under no obligation within the Digital Identity Ecosystem to proactively notify any Requesting Organization that has previously received the Subject-Specific Personal Information, nor to flag that a change has been made, unless required by law. The onus is on a Requesting Organization to compare newly received data against previously received data for changes, and act on changes as relevant to their business processes.

4.3. Upstream and Downstream Handling of Personal Information

The handling of Personal Information by a Disclosing Organization is subject to relevant privacy legislation and regulations and is not generally deemed to fall within the scope of the requirements of the PCTF until that data is processed for the purpose of sharing via the Digital Identity Ecosystem. An exception to this is when a Requesting Organization has specific requirements on the handling of Personal Information by its source (the Disclosing Organization). These requirements will thus form part of the Digital Identity Ecosystem governance and constitute "upstream" requirements with

which any Disclosing Organization servicing that Requesting Organization must comply. Similarly, the handling of Personal Information by a Requesting Organization is subject to relevant privacy legislation and regulations and is not generally deemed to fall within the scope of the requirements of the PCTF once that data has been shared via the Digital Identity Ecosystem. An exception to this is when a Disclosing Organization has specific requirements on the handling of Personal Information by its destination (the Requesting Organization). These requirements will thus form part of the Digital Identity Ecosystem governance and constitute "downstream" requirements with which any Requesting Organization receiving data from that Disclosing Organization must comply.

4.4. Privacy by Design

Privacy by design is one of DIACC's guiding principles for a Canadian Digital Identity Ecosystem, specifically "To, Implement, protect, and enhance privacy by design". Privacy considerations are integral to and should be taken into account at all stages of the development of a digital identity solution. Privacy-enhancing tools enable an individual to manage their information and what specified purpose(s) it is used for.

While the House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI), has recommended that PIPEDA be amended to include privacy by design principles [2], the current PIPEDA Fair Principles do not explicitly address privacy by design. As such, the Conformance Criteria of the PCTF Privacy Component do not include criteria to evaluate adherence to privacy by design.

5. 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.

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.

Note: PCTF 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.

"Participants" refer to each of the Disclosing Organization, Requesting Organization, Notice and Consent Processor, Network Facilitator and the Governing Body roles. See the Privacy Overview for definitions of these roles. Depending on the use case, separate organizations or persons may take on one or more roles. They are not intended to imply any particular solution, architecture or implementation.

5.1 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 the requirement is expected to be met, except in limited cases where the applicant documents valid reasons or circumstances to ignore the requirement. The full implications of such an exception must be understood and carefully weighed before choosing to not adhere to the conformance criteria as described.

- **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.

6. 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, Network Facilitators, Notice and Consent Processors, and the Governing Body **MUST** have in place a privacy management program that documents policies, practices and procedures to comply with applicable privacy laws, and incorporates the following: • What information they collect, use, keep and disclose and why • Privacy risk assessment • Individual rights, complaints and questions • Any relevant restrictions on collection, use, retention or disclosure (legal, contractual) • Training and awareness • Diligence on third parties (includes customer, suppliers, service providers, partners) • Security measures and incident response and management • Information about cross-border transfer of personal information
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 reviews of personal information handling practices (including those related to the provision of notice and the obtaining of consent), and has the authority to intervene on privacy issues specifically relating to the organization's role as a Disclosing Organization, Requesting Organization, Notice and Consent Processor, Network Facilitator, or Governing Bod
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 perform an independent internal or external review of their personal information management practices (including its notice and consent management practices), with a maximum of 1 year between reviews, to verify that Personal Information is being handled in the way described by its privacy policy.
5	Participants **MUST** maintain evidence of compliance to the conformance criteria for Principles 1-10, which can be provided to other Participants, including the Governing Body, when requested.
6	As part of their privacy management programs, Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, Network Facilitators and the Governing Body **MUST** have and periodically test processes to manage Personal Information breaches or breaches of confidentiality, which includes assessing damage or harm (for organizations and individuals), reporting, containment, remediation, notification, and prevention steps.
7	The Governing Body **MUST** clearly define, document 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]
1	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.

2	The Governing Body **MUST** define and document procedures and policy that: • investigate and manage deviations from Principles 1-10 by organizations operating within the Digital Identity Ecosystem, including assessing the risk to Subjects and that breaches are reported by Participants to relevant privacy regulators and Subjects • if applicable, verify that specific requirements defined by an organization on 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 • 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]
1	The Disclosing Organization **MUST** be able to demonstrate that sufficient due diligence was performed over the existence of relevant governance or control-processes at 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 that includes information request records 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** have a clear, defined, justifiable identity-related 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 1 year between reviews, perform an internal review of their Personal Information collection and use requirements, and update future requests accordingly.

6	The Requesting Organization **MUST** verify that the reasons for the collection and use of Subject-Specific Personal Information are clear, specific, and unambiguous.
7	Before or when any Personal Information is collected, the Notice and Consent Processor **MUST** explain explicitly 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.
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]
1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** verify that the notice and knowledge required for the consent request is clear, understandable and meaningful to the User, and include details to indicate if the consent is one-time only or ongoing, and how the User may revoke or withdraw the consent. See also NOTI 1, 3, 4 and 5, CONS-8 and MANA-2 and 6 in the PCTF Notice and Consent component.
2	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** ensure the consent process is clear as to what is being consented to. In all cases, a straightforward means **SHOULD** be provided for the User to get additional information, as may be required.
3	The Disclosing and the Requesting Organizations **MUST** verify that the Notice and Consent Processor performs its function of providing notice, and obtaining, recording and managing consent appropriately prior to disclosing or receiving the Subject-Specific Personal Information. Both the Disclosing and the Requesting Organizations **MUST** ensure that the consent is in place before providing it or before receiving it. See also NOTI-1 in the PCTF Notice and Consent component.
4	The Disclosing Organization **MUST** verify that evidence of the notice and consent is obtained by the Notice and Consent Processor and then stored as a Notice and Consent record.

5	The Disclosing Organization **MUST** verify that 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** define the purpose of processing the Subject-Specific Personal Information requested in the content of the notice. See also NOTI-3 in the PCTF Notice and Consent component.
8	The Requesting Organization, as the originator of the request for consent, **MUST** define whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure in the content of the notice. See also NOTI-3 in the PCTF Notice and Consent component.
9	The Requesting Organization **MUST** ensure that the consent request follows a principle of minimal disclosure.
10	The Requesting Organization **MUST** verify that a record of the notice and consent is obtained by the Notice and Consent Processor and then stored as a Notice and Consent record.
11	When the Requesting Organization is made aware that consent is no longer valid, the Requesting Organization **MUST** have a documented process to cease further collection of Subject-Specific Personal Information based on this invalidated consent. See also MANA-2 in the PCTF Notice and Consent component.
12	The Notice and Consent Processor **MUST** provide notice to the User within the Digital Identity Ecosystem.
13	The Notice and Consent Processor **MUST** verify that the notice clearly states whether the request is for a one-time disclosure of the personal information or to allow on-going disclosure within the Digital Identity Ecosystem.
14	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.

15	The Disclosing Organization **MUST** define the sensitivity of the Personal Information being shared and stipulate controls (e.g., masking policies or other safeguards) for the display of sensitive information within the notice.
16	If the Notice and Consent Processor displays Personal Information in the notice statement, the Personal Information **MUST** be displayed in accordance with any controls (e.g., masking policies or other safeguards) stipulated by the Disclosing Organization. See NOTI-3 in the PCTF Notice and Consent component for types of information that may be required in the notice statement.
17	The Notice and Consent Processor **MUST** have a documented process to collect consent and communicate this consent to the Disclosing Organization and Requesting Organization involved in the digital identity transaction. See also RECO 2 in the PCTF Notice and Consent component.
18	The Notice and Consent Processor **MUST** record the consent decision. See also RECO-1 in the PCTF Notice and Consent component.
19	The Notice and Consent Processor **SHOULD** have a straightforward, documented process for the User to review and manage any consents given. See also MANA 7 in the PCTF Notice and Consent component.
20	For identity transactions where consent is being managed between multiple Requesting Organizations and Disclosing Organizations, the Notice and Consent Processor **MUST** ensure that processing is conducted in accordance with the purpose specified in the Notice and the consent granted by the User for each organization.
21	The Notice and Consent Processor **MUST** have processes 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. See also MANA-3, 4 and 5 in the PCTF Notice and Consent component.
22	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.
23	The Governing Body **MUST** define guidelines on the formulation of notices and collection of consent, to provide a consistent and optimized user experience across the Digital Identity Ecosystem.

24	The Governing body **MUST** 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]
1	The Disclosing Organization **MUST** establish a documented process to verify that the Requesting Organization has a clear, defined, justifiable identity-related purpose for collecting the requested Personal Information.
2	The Requesting Organization **MUST** only use, keep and disclose the Personal Information for identity-related purpose(s), such as validation or verification of identity attributes of an applicant for a service. They **MUST NOT** use that identity information for other unrelated purposes, such as marketing, without consent.
3	The Requesting Organization **MUST** limit the Personal Information that is collected via the Digital Identity Ecosystem to that which is required to fulfill the stated identity-related purpose(s).
4	The Requesting Organization **MUST** publicly document, or make available, in clear and unambiguous language the nature and purpose of Personal Information collected.
5	The Requesting Organization **MUST** educate applicable employees on the nature and purpose of Personal Information collected in order to accurately respond to any third party inquiries, when they are required to do so.
6	The Notice and Consent Processor **MUST** verify that Personal Information being collected is limited to only that which is required to perform the relevant notice and consent function.
7	The Network Facilitator **MUST NOT** collect Personal Information beyond that which is required to support their service agreements. For example, acting on their behalf as a service or network provider.
8	The Governing Body **MUST** have a documented process that would review the Requesting Organization's reason for collecting the requested Personal Information, and review that the collection is fair and lawful.
9	The Governing Body **MUST** provide guidelines on appropriate ways to limit collection of Personal Information within and by the Digital Identity Ecosystem Participants.

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]
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	The Disclosing Organization **MUST** comply with the defined minimum and maximum data retention policy~~, if specified,~~ for the Digital Identity Ecosystem, 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 that which is required to fulfill the stated identity-related purpose(s) in alignment with Subject's consent, unless otherwise permitted or required by law.
5	The Disclosing Organization **MUST** have processes in place to ensure that Personal Information to be disclosed is accurate, complete and as up-to-date as possible.
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** implement maximum and minimum valid retention periods of the Subject-Specific Personal Information received via the Digital Identity Ecosystem, and be consistent with the retention specified in the Notice. See also NOTI-3 in the PCTF Notice and Consent component.
8	The Requesting Organization **MUST** obtain consent on the use or retention of the Subject-Specific Personal Information (received through the Digital Identity Ecosystem) for purposes beyond that specified through the Notice and Consent Processor at the time of collection. See PCTF Privacy Overview for definition of consent in the context of PCTF Privacy component.
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. Note: Typically, 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	Requesting Organizations and Notice and Consent Processors **MUST** dispose of personal information after the retention period expires. See also MANA-2 in the PCTF Notice and Consent component.
12	The Network Facilitator **MUST NOT** use, disclose or retain Personal Information beyond that which is required to support their service agreements. For example, acting on their behalf as a service or network provider.
13	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.
14	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.
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]
1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** ensure that Users have an ability to update their inaccurate or outdated Personal Information held by the respective Participant of the Digital Identity Ecosystem. For example, a consumer-focused identity provider may provide the User with the ability to directly update their Personal Information at any time.

2	The Disclosing Organization **MUST** implement policies, procedures, and systems to identify, correct and manage (e.g., updating Subject records) inaccurate or outdated Personal Information. Note: Typically, 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. For example, 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 Personal Information that is obtained from other Participants of the Digital Identity Ecosystem conflicts with Personal Information that is held by the Requesting Organization, the Requesting Organization **MUST** have a documented procedure to resolve the discrepancy.

8	The Notice and Consent Processor **MUST** store an audit trail of notices presented and consent decisions received, and when this was provided. 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 policy and guidelines for ensuring accuracy of Personal Information within the Digital Identity Ecosystem. For example, this may include guidance for implementing services that allow (with the Subject's consent) broadcast of updates to Requesting Organizations who have subscribed to receive such updates.
SAFE	**Principle 7 - Safeguards** *Personal information must be protected by appropriate security relative to the sensitivity of the information.*[1]
1	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** have security policies, processes, controls and measures in place to protect Personal Information and are communicated to the User (as appropriate).
2	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **MUST** implement policies, processes and controls to identify, manage and mitigate security incidents and breaches, including reporting externally to other organizations, regulators, the Governing Body, or Users, as necessary, appropriate or legally required.
3	The Disclosing Organization **MUST** develop and implement a security policy that specifically includes protections applied when disclosing Subject-Specific Personal Information in the context of the Digital Identity Ecosystem.
4	The Disclosing Organization and Requesting Organization **MUST** implement security safeguards, appropriate to the risk of harm and sensitivity of Personal Information identified in risk assessment (threat risk assessment and/or privacy impact assessment as appropriate), to protect access to Personal Information.
5	The Disclosing Organization and Requesting Organization **MUST** implement security safeguards to protect access to Personal Information both at rest and in transit.
6	The Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, and Network Facilitators **MUST** conduct a regular review and update of their security measures relating to the Digital Identity Ecosystem.

7	The Requesting Organization **MUST** develop and implement a security policy to protect Personal Information that specifically includes protections applied when receiving Personal Information in the context of the Digital Identity Ecosystem.
8	The Notice and Consent Processor and Network Facilitator **MUST** implement security safeguards as specified in relevant criteria in the PCTF Infrastructure (Technology & Operations) component.
9	The Notice and Consent Processor **MUST** implement security safeguards appropriate to the sensitivity of any Personal Information presented to the Subject in the privacy notice, and to the risk of harm identified in risk assessment (threat risk assessment and/or privacy impact assessment as appropriate), to protect access to Personal Information.
10	The Network Facilitator **MUST** develop and implement a security policy appropriate to the function of the network. Typically, this will involve ensuring that the Network Facilitator minimizes its visibility of Personal Information.
11	The Governing Body **MUST** define and 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.
12	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]

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 (which may reference information maintained by the Governing Body) • what personal information is collected, used, retained or disclosed • the purposes for the collection, use, retention or disclosure • the names or categories of third-party recipients of personal information • an explanation of the Subjects's privacy rights and how to exercise them • how the Subject's personal information is protected • where to go for more information • who to contact for help
2	Disclosing Organizations, Requesting Organizations, and Notice and Consent Processors **MUST** have a documented process to 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	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, and Network Facilitators **MUST** have a documented process to provide information to Users concerning their role in the Digital Identity Ecosystem following the Governing Body guidelines, when requested.
4	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, and Network Facilitators **MUST** ensure information concerning their role is clearly delineated from other services and functions provided by the organization (that are not part of the Digital Identity Ecosystem per se), such as marketing.
5	The Governing Body **MUST** develop and maintain clear and understandable information about how, in general terms, personal information is collected, used and disclosed within the Digital Identity Ecosystem and how Users can exercise their privacy rights.
6	The Governing Body **MUST** have a documented procedure to review a Participant's privacy policy and practices information required by the Principle 8 Openness criteria, and that such information is presented in a consistent manner to avoid conflicting or confusing messages.

7	The Governing Body **MUST** provide guidelines to Participants on compliance with the criteria statements in this Principle 8 - Openness section within the Digital Identity Ecosystem.
8	The Governing Body **MUST** verify that each Participant, including the Governing Body, has 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]
1	Participants in the Digital Identity Ecosystem **MUST** have appropriate policies concerning the existence, use, and disclosure of Personal Information.
2	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** have appropriate processes to manage complaints and rights-requests from Users including: • clearly setting out the responsibilities of other entities involved for resolution • training applicable staff to be able to respond to any requests or complaints
3	Disclosing Organizations, Requesting Organizations and Notice and Consent Processors **SHOULD** provide inbuilt features that automatically provide the User with the ability to access and correct their personal information. Note: Because the Notice and Consent Processor facilitates the sharing of, but does not use, Personal Information, the "individual access" is likely to be limited to viewing the audit trail of Notice and Consent activities relating to the Subject.

4	Where Disclosing Organizations, Requesting Organizations and Notice and Consent Processors do not provide inbuilt features, they **MUST** create a documented process for Users to obtain information concerning the existence, use and disclosure of their Personal Information, and make this clear to Users. Note: Because the Notice and Consent Processor facilitates the sharing of, but does not use, Personal Information, the "individual access" is likely to be limited to viewing the audit trail of Notice and Consent activities relating to the Subject.
5	If the Requesting Organization determines that the Personal Information it receives from the Digital Identity Ecosystem is inaccurate or incomplete, processes **SHOULD** exist to notify the relevant Disclosing Organization of the problem.
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 they **MUST** comply with criteria INDI 1 through 4.
7	The Governing Body governance arrangements **MUST** include a section on Principle 9 "Individual Access" processes and guidelines that are provided to Participants and that are 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]
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 clearly available for anyone requesting it.

2	Disclosing Organizations, Requesting Organizations, Notice and Consent Processors, and Network Facilitators each **MUST** have a compliance management program that includes at least: • 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** provide guidelines to Participants on how to notify and respond to complaints in a timely manner as well as record actions in order that the Subject is provided with the necessary support from the correct Participant, as efficiently and clearly as possible.

7. Notes and Assumptions

More than one organization may be responsible for carrying out the Privacy trusted processes from end-to-end. The involvement of several organizations or persons may introduce complexity in the assessment and certification process, but the trust framework does not constrain different implementation approaches. Within the conformance profile three organizational roles are defined (requesting organization, disclosing organization and notice and consent processor). These help to isolate the different functions and responsibilities within the end-to-end process. They are not however intended to imply any particular solution, architecture or implementation.

Privacy-respecting practices rely on the principle that individuals know and understand the details and potential benefits and consequences associated with managing their personal information, and can take action based on that information. The specific requirements for this are addressed in the Notice and Consent PCTF Profile.

8. References

This section lists the external standards, guidelines, and other documents referenced in the PCTF Privacy component.

1. PIPEDA fair information principles, Office of the Privacy Commissioner of Canada, Revised: May 2019 and Schedule 1 of the Government of Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96

2. Report of the Standing Committee on Access to Information, Privacy and Ethics, February 2018, Recommendation 14, p. 52

9. Revision History

Version Number	Date of Issue	Author(s)	Brief Description
0.01	2018-10-31	Consult Hyperion	Initial working draft
0.02	2018-11-22	DIACC	Terms for roles changed: • "Network" to "Network Provider' • "Eco-System" to "Governing Body"
0.03	2019-03-20	PCTF Editing Team	Updates for the discussion draft • Removed notice and consent content • Privacy principles • Describe the purpose of Privacy component
0.04	2019-05-09	PCTF Editing Team	Updated Privacy key component's descriptions
0.05	2019-06-26	PCTF Editing Team	Incorporated comments from discussion draft TFEC review
0.06	2019-10-31	Privacy Design and PCTF Editing Teams	Revised content based on discussion draft open review comments.
0.07	2019-11-22	PCTF Editing Team	Applied standard outline for PCTF Overview, which consolidates conceptual information in the Overview.
0.08	2019-12-11	PCTF Editing Team	Updated from Privacy design team meetings.
0.09	2020-01-02	PCTF Editing Team	Updated based on suggested editorial changes from open review.
0.10	2020-02-12	PCTF Editing Team	Updated based on several consultation sessions with TFEC expert team to review received TFEC comments
1.0	2020-02-12	PCTF Editing Team	Approved as Draft Recommendation V1.0

1.1	2021-10-29	PCTF Editor and Privacy Design Team	Updated in response to public comments
1.1	2021-11-10	PCTF Editor and Privacy Design Team	TFEC approves as a Candidate for Final Recommendation V1.1
1.2	2022-02-05	PCTF Editor and Privacy Design Team	Updated as per Privacy Design Team based on comments from public review
1.2	2022-03-02	PCTF Editor and Privacy Design Team	TFEC approves as a Candidate for Final Recommendation V1.2
1.2	2022-03-18	PCTF Editor and Privacy Design Team	Approved as Final Recommendation V1.2 through DIACC Sustaining Member Ballot