PCTF Infrastructure (Technology & Operations) Conformance Profile Draft Recommendation V1.0

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

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

Forthcoming PCTF releases will expand, clarify, and refine the content of this document.

Table of Contents

1. Introduction to the PCTF Infrastructure (Technology & Operations) Conformance Profile

This document specifies the Conformance Criteria of the PCTF Infrastructure (Technology & Operations) 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 Infrastructure Component specify the characteristics of the technology and technology operations supporting the implementation of systems delivering service compliant with PCTF Profiles. The criteria are expressed in generic terms, recognizing that specific technologies or technology characteristics (e.g. protocols) are likely to be mandated, and will vary, within each individual Digital Identity Ecosystem.

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

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.

1.2. Infrastructure Conventions

Each PCTF component includes conventions that ensure consistent use and interpretation of terms and concepts appearing in the component. **The PCTF Infrastructure (Technology & Operations) Component Overview provides conventions for this component**. These conventions include definitions and descriptions of the following items that are referred to in this conformance profile:

- Key terms and concepts
- Abbreviation and acronyms

Notes:

- Conventions may vary between PCTF components. Readers are encouraged to review the conventions for each PCTF component they are reading.
- Defined Terms – For purposes of this conformance profile, terms and definitions listed in both the PCTF Infrastructure Component Overview and the PCTF Glossary apply. Key

terms and concepts described and defined in this section, or the PCTF Infrastructure Component Overview, or the PCTF Glossary are capitalized throughout this document.

- Hypertext Links – Hypertext links may be embedded in electronic versions of this document. All links were accessible at time of writing.

2. Infrastructure Component Conformance Criteria

The Conformance Criteria listed below are organized into three broad categories. These are:

- POL – policy and plan requirements defining and supporting the technology architecture under which the system components participating in the Digital Identity Ecosystem operate.
- TECH – technology related requirements
- OPS – technology operations related requirements

For ease of use, the Criteria are numbered within their section and may be referred to using these identifiers (e.g. The first criterion in the POL section may be referenced as POL-1).

Criteria scope may be assumed to apply only to the technology or system components leveraged by an organization in its provision or consumption of service within a Digital Identity Ecosystem.

Note: A PCTF Working Group on LoA is underway with the objective of defining how LoA will be treated across all PCTF Profiles. Treatment of potential variances in Conformance Criteria based on Service LoA were deferred in this version of the Profile. Please reserve your comments in this area to an enhanced draft of these documents when the LoA Working Group has published their results.

Reference	Conformance Criteria
POL	**Requirements relating to the technology policies and plans required to support the infrastructure leveraged to service the Digital Identity Ecosystem.**

92		Policies and plans **MUST** be developed, documented, and disseminated within the organization that address: • Risk Assessment; • Audit and accountability; • Disaster or contingency planning; • Identification and authorization; • Systems and communication protection; • Incident response; • System and information integrity; • Information management; • System maintenance; • Technical access control (e.g. lockdown of operating systems, intrusion detection, password management, encryption, and network access management); • Physical access to technology assets; and • Human resource management as it pertains to personnel interacting with the security infrastructure.
93		Technology management or technical operations policies and plans **MUST** be reviewed and updated regularly, on a fixed schedule appropriate to the operational context of the enterprise. Ad hoc adjustments **MAY** also be made when business conditions warrant them. A technology management plan **MUST** be developed covering all technologies, system components, integrations and information exchanges leveraged in the delivery of service to the Digital Identity Ecosystem. The technology management plan **SHOULD**: • Be consistent with the organization's enterprise architecture; • Define asset lifecycle management practices; • Describe capacity and utilization management practice; • Describe performance management testing practices and metrics; • Describe the requirements for the information system and its relationships with or connections to other information systems; • Ensure alignment with related areas in other plan artefacts (e.g. risk management, security, change management); • Identify key risks and their business or operational impact; • Demonstrate alignment with an industry standard service management framework (e.g. ITIL). This **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements. Finally, there **MUST** be a process to ensure that changes to the technology management plan are reflected in the implementation of related system components.

94		An information security architecture for information systems providing service to the Digital Identity Ecosystem **MUST** be formally developed. This **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements. Finally, there **MUST** be a process to ensure that changes to the information security architecture are reflected in related security and operational plans.
95		A security plan **MUST** be developed covering all technologies, system components, integrations and information exchanges leveraged in the delivery of service to the Digital Identity Ecosystem. The security plan **SHOULD**: • Be consistent with the organization's enterprise architecture; • Define the authorization boundary for the system; • Describe the operational context of the information system; • Provide the security categorization of the information system and its data; • Describe the operational environment for the information system and relationships with or connections to other information systems; • Provide an overview of the security requirements for the system; • Identify key risks and their business or operational impact; • Describe the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; This **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements. Finally, there **MUST** be a process to ensure that changes to the security plan are reflected in the implementation of related system components.
96		An incident response plan **MUST** be developed covering security incidents applicable to all technologies, system components, integrations and information exchanges leveraged in the delivery of service to the Digital Identity Ecosystem. The incident response plan **SHOULD**: • Provide a roadmap for implementing its incident response capability; • Meet the unique requirements of the organization, which relate to mission, size, structure, and functions; • Define reportable incidents; • Provide metrics for measuring the incident response capability within the organization; • Define the resources and management support needed to effectively maintain the incident response capability; This **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements. Finally, there **MUST** be a process to ensure that changes to the incident response plan are reflected in the implementation of related system components.

97		A contingency plan (sometimes referred to as a disaster recovery plan) **MUST** be developed covering all technologies, system components, integrations and information exchanges leveraged in the delivery of service to the Digital Identity Ecosystem. The contingency plan **SHOULD**: • Identify essential missions and business functions and associated contingency requirements; • Provide recovery objectives, restoration priorities, and metrics; • Address contingency roles, responsibilities, assigned individuals with contact information; • Address maintenance of essential missions and business functions despite an information system disruption, compromise, or failure; • Address eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and • Include descriptions of alternate resources including physical site, telecommunication services, storage, and computing resources. This **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements. Finally, there **MUST** be a process to ensure that changes to the contingency plan are reflected in the implementation of related system components.
98		A configuration management plan **MUST** be developed covering all technologies, system components, integrations and information exchanges leveraged in the delivery of service to the Digital Identity Ecosystem. The configuration management plan **SHOULD**: • Address roles, responsibilities, and configuration management processes and procedures; • Establish a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; • Define the configuration items, and any related baselines, to be managed under the plan. This **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements. Finally, there **MUST** be a process to ensure that changes to the configuration management plan are reflected in the management of related system components.

99		There **SHOULD** be a formal continuous monitoring plan and continuous monitoring program that includes: • Identification of the metrics to be monitored; • Establishes frequency for monitoring; • Security status monitoring • Response actions to address results of the analysis of security-related information; and • Reporting the security status of organization and the information system.
100		A security and privacy assessment plan **MUST** be developed covering all technologies, system components, integrations and information exchanges leveraged in the delivery of service to the Digital Identity Ecosystem. The security assessment plan **SHOULD**: • Identify the security controls and control enhancements under assessment; • Define assessment procedures to be used to determine security control effectiveness; • Identify the assessment environment, assessment team, and assessment roles and responsibilities; • Define the metrics to be evaluated; • Define a security assessment report that documents the results of the assessment; and • Identify the privacy safeguards in place, and their controls (Please refer to the Safeguards section of the PCTF Privacy Conformance Profile for additional detail in this area). This **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements. Finally, there **MUST** be a process to ensure that changes to the security and privacy assessment plan are reflected in the configuration of related system components.
101		There **MUST** be an operational standard requiring developers to follow a documented development process that explicitly addresses security requirements, identifies the technology standards and toolsets to be used, and identifies the specific work tool configurations to be used.
102		There **SHOULD** exist a formal elaboration of business capability/service architecture that is reviewed and updated.
103		There **SHOULD** be documented policies establishing usage restrictions, configuration/connection requirements, and implementation guidance for: • wireless access; • mobile device access; and • remote user access.

104			A security and business activity audit plan **MUST** be developed covering all technologies, system components, integrations and information exchanges leveraged in the delivery of service to the Digital Identity Ecosystem. The audit plan **SHOULD**: • Identify the events for which audit information must be captured; • Determine that the system components are capable of capturing auditable events; and • Provide rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents. This **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements. Finally, there **MUST** be a process to ensure that changes to the audit plan are aligned with the evolution of related system components.
105			A risk assessment audit plan **MUST** be developed covering all technologies, system components, integrations and information exchanges leveraged in the delivery of service to the Digital Identity Ecosystem. The risk assessment plan **SHOULD**: • Govern the assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; • Define the documentation of risk assessment results; • Define the roles and responsibilities for the dissemination of risk assessment results This **MUST** be reviewed and updated on a continuous basis to reflect evolving business or operational requirements.
106	**TECH**		**Technology requirements required by organizations servicing the Digital Identity Ecosystem**
107			The organization **MUST** deploy and manage the specific tools, software, security devices and protocols, network architecture, and communication protocols mandated by the Digital Identity Ecosystem they wish to operate in.
108			Tools and techniques **MUST** be in place that provide malicious code protection mechanisms at information system entry and exit points (e.g. firewalls, gateways, host intrusion detection systems) to detect and eradicate malicious code. These tools **SHOULD** automatically update malicious code protection mechanisms.
109			The information system **MUST** ensure the confidentiality and integrity of Digital Identity information at rest and in transit. Please refer to the PCTF Privacy Conformance Profile for additional related requirements in this area.

110		The information system **MUST** ensure the authenticity of communications sessions (e.g. unique randomized session identifiers, session identifier invalidation upon logout, proper application of approved encryption certificates based on enterprise policy).
111		The information system **MUST** invalidate session identifiers upon user logout or other session termination. Please also refer to the Session Termination section of the PCTF Authentication Conformance Profile for additional context.
112		The organization **MUST** issue public key certificates in accordance with organization defined certificate policy or obtain public key certificates from a well known, public trust anchor certificate authority.
113		The information system MUST terminate the network connection associated with a user session, or system-to-system communication session, at the end of the session or after a predefined period of inactivity.
114		The organization **SHOULD** employ integrity verification tools to detect unauthorized changes to software, firmware, and information.
115		Tools **MUST** be in place to monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.
116		Monitoring and alarming tools, devices, and techniques **MUST** be employed that will monitors the information system to detect: • Attacks and indicators of potential attacks; and • Unauthorized local, network, and remote connections. See also the Monitoring section of the PCTF Authentication Conformance Profile for additional information.
117		The information systems that collectively provide name/address resolution service for an organization **MUST** be fault-tolerant and implement internal/external role separation.
118		The organization **MUST** establish and manage cryptographic keys that meet required cryptography standards employed within the information system.
119		Boundary protection tools, devices, and techniques **MUST** be employed that will: • Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; • Implement subnetworks for publicly accessible system components that are logically separated from internal organizational networks; and • Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

120		The organization **MUST** employ tools and techniques to protect against or limit the effects of denial of service attacks.
121		The information system **MUST** uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).
122		The organization **MUST** ensure that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. Please refer to the credential issuance and authentication sections of the PCTF Authentication Conformance profile for additional guidance.
123		The organization **SHOULD** employ automated tools to determine if password authenticators are sufficiently strong to satisfy the requirements of the organization's security policy. Please refer to the credential issuance and authentication sections of the PCTF Authentication Conformance profile for additional guidance.
124		The organization **MUST** implement multifactor authentication for remote access to privileged and non-privileged accounts such that one of the factors is provided by a device separate from the system gaining access.
125		The organization **MUST** implement tools to defend against authentication replay and secret guessing attacks to gain network access. See also the Threat Mitigation section of the PCTF Authentication Conformance Profile.
126		The organization **MUST** analyze changes to the information system to determine potential security impacts prior to change implementation.
127		The organization **MUST** have automated intrusion detection and alerting technology in place for all technology components leveraged in the delivery or consumption of digital identity
128		The organization **MUST** proactively assess and maintain the adequacy of systems and services, including system resource levels and the currency of hardware and operating system patch levels.
129		The information system **SHOULD** have security safeguards to protect its memory from unauthorized code execution.
130		The information system **MUST** deploy cryptographic tools and other data protection methods and technology to ensure privacy is maintained during information exchanges. Please refer to the PCTF Privacy Conformance Profile for additional information. Cryptographic tools **SHOULD** meet an industry recognized validation standard (e.g. FIPS 140-2 or equivalent).
131	**OPS**	**Operational requirements for organizations servicing the Digital Identity Ecosystem.**
132		The organization **MUST** manage the system components using its defined system development life cycle that incorporates security concerns.
133		The organization **MUST** have formal information retention and disposition schedules subject to monitoring and audit to ensure compliance.

134		Formal enterprise technology governance systems and processes (e.g. governance task and workflow management, change management) **SHOULD** be in place. These **SHOULD** include ongoing monitoring and activity audit controls to ensure compliance.
135		The organization **MUST** provide the capability to restore information system components within restoration time periods as defined in the contingency plan. This capability **MUST** encompass recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
136		Full testing, evaluation, and update of the contingency plan **MUST** be performed on a regular (e.g. biennial, annual preferred) basis.
137		Comprehensive automated backup procedures **MUST** be in place. This capability includes backup of: • User level information • System level information • System and security documentation
138		Automated system-wide backup procedures in operation **MUST** align with the contingency plan.
139		Backups of critical system software and operational data **SHOULD** be stored in a facility that is physically separate from the operational system. Processes and procedures **MUST** be in place to protect the confidentiality, integrity, and availability of backup information at storage locations in alignment with governance and risk management policy.
140		There **MUST** be a program of continuous vulnerability testing of system and software components leveraged in the delivery of services to the Digital Identity Ecosystem. Vulnerability scanning techniques, and tools that readily update the vulnerabilities to be scanned, **SHOULD** be employed and operated in an automated fashion.
141		The organization **MUST** conduct regular penetration testing of all components leveraged in the delivery of services to the Digital Identity Ecosystem.
142		Remote access methods **MUST** be controlled and monitored.
143		Remote access **MUST** be routed through managed network access control points.
144		There **SHOULD** be automated systems (e.g. provisioning, rights assignment and management) to support the management of information system accounts.
145		Processes **MUST** be in place to automatically disable inactive accounts after a defined period of inactivity based on information system control policy.
146		There **MUST** be a system record automatically created for account creation, modification, enabling, disabling, and removal actions.

147		Controls **MUST** be in place to require system accounts to log out after a specified period of inactivity.
148		Privileged user accounts **MUST** be established and administered using a role-based access scheme.
149		A documented policy **MUST** be in place and its adherence monitored for the use of shared groups or accounts.
150		Automated processes **MUST** be in place to terminate shared/group account credentials when members leave the group.
151		Automated processes **MUST** be in place to enforce a limit of unsuccessful login attempts and lock the account/node until released by an administrator or administrative process (e.g. forced password reset).
152		The system **MUST** prevent system access after a defined period of inactivity and require that the user re-establishes access using established identification and authentication procedures. Please refer also to the Session Timeout criteria defined in the PCTF Authentication Profile for additional information.
153		Processes **MUST** be in place to limit the number of concurrent sessions for each defined account type as per the organization's established security and access policy.
154		Organizations **MUST** assign account managers for information system accounts and establish formal conditions for group and role membership granting access authorizations. Documented processes **MUST** be in place requiring approvals for account creation and have automated procedures to monitor information system account usage.
155		The organization **MUST** employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. This includes: • Configuration of software products to reflect the most restrictive mode consistent with operational requirements; • Restricted access to Digital Identity data using configurations that provide explicit access to only that data required by the individual or system that requires it; and • Network and communication device configurations restricting access to only those system components or services that are required.
156		The organization **MUST** maintain availability of information in the event of the loss of cryptographic keys by users.
157		The information system **MUST** implement cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to Digital Identity information during transmission.

158		The organization **MUST** authorize external connections between information systems based on formal security agreements as defined in the organization's security policy. For each individual connection the interface characteristics, security requirements, and the nature of the information communicated **MUST** be documented. Change history for either the agreement or interface characteristics **SHOULD** be maintained.
159		Internal connections between information system components **MUST** be documented, capturing the interface characteristics, security requirements, and the nature of the information communicated. Change history for the interface characteristics **SHOULD** be maintained.
160		Processes **MUST** be in place to ensure approved authorizations for controlling the flow of information within the system and between interconnected systems based on the organization's security policy
161		The organization **SHOULD** employ automated mechanisms to make security alert and advisory information available throughout the organization.
162		The organization **SHOULD** receive information system security alerts, advisories, and directives from a recognized authority on an ongoing basis and generate internal security alerts, advisories, and directives as deemed necessary.
163		The organization **MUST:** • Identify, report, and correct information system flaws; • Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; • Install security-relevant software and firmware updates within a time period, after release, defined by the organization's security policy; and • Incorporate flaw remediation into the organizational configuration management process.
164		Formal technology change management processes **MUST** be in place to evaluate and manage risk associated with technology evolution.
165		The organization **MUST** define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system.

166		Technology change management processes **SHOULD**: • Determine the types of changes to the information system that are configuration-controlled; • Review proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses; • Document configuration change decisions associated with the information system; • Implement approved changes to the information system; • Retain records of changes to the information systems for the time period specified in the change control policy; and • Coordinate and provide oversight for configuration change control activities through a formally constituted change control governance body
167		Activity monitoring and audit trail facilities **MUST** be in place to provide a record of all digital identity related transactions within the Digital Identity Ecosystem. Further, these audit trails must be protected from alteration and limited access policies enforced.
168		Audit information and audit tools **MUST** be protected from unauthorized access, modification, and deletion.
169		The information system **MUST** have mechanisms in place that protect against an individual (or process acting on behalf of an individual) falsely denying having performed actions to be covered by non-repudiation.
170		Audit records **MUST** be securely retained for the time period identified in the organization's information retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
171		Audit records **MUST** be generated for Digital Identity transactions containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
172		Audit records **MUST** be generated for the execution of privileged system functions.
173		Processes **MUST** be in place to prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.
174		Information system account usage **MUST** be monitored for atypical usage and atypical usage patterns reported and/or accounts disabled dependent on risk associated with observed atypical usage.
175		Processes **MUST** be in place to enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.

176		The organization **SHOULD** have clearly identified data and information stewards
177		The organization **SHOULD** have a documented API standard