TRUST CENTRE

Cloud Hosting & Delivery Policy

HOSTING, SECURITY, AVAILABILITY, SUPPORT AND SERVICE OPERATIONS

Effective Date: 6 October 2025
Classification: Public
Document ID: PCL-TRUST-CHD-013

This document is intended for public distribution. Supporting assurance evidence, detailed architecture, system configurations and customer-specific service records may be subject to separate access and confidentiality restrictions.

Contents

This policy should be read together with the applicable customer agreement, Ordering Document, Cloud Service Description, Data Processing Addendum, support terms and referenced Trust Centre policies.

1. Overview

This policy describes PCL One's baseline practices for hosting, securing, operating, monitoring, maintaining and supporting in-scope PCL One-managed Cloud Services. It brings together the service-delivery controls that apply across the hosting lifecycle while preserving the more detailed commitments contained in the applicable customer agreement, Ordering Document, service schedule, Data Processing Addendum and Trust Centre policies.

POLICY STATUS

This is a public baseline policy. Service-specific commitments are governed by the applicable agreement, Ordering Document, Cloud Service Description, service schedule, Data Processing Addendum and support terms. Where a customer-specific document contains a more specific or stricter commitment, that customer-specific commitment governs for the relevant service.

2. Scope and applicability

- Applies to PCL One-managed cloud production services and the PCL One-managed components used to deliver them.
- Covers hosting, infrastructure dependencies, security administration, backup and recovery, monitoring, planned change, maintenance, support coordination, incident handling and service exit.
- Applies to production and, where relevant, non-production environments identified in the applicable service design or Order.
- Does not make customer-managed systems, unrelated third-party services or unsupported integrations part of the PCL One-managed service boundary unless expressly included in the applicable Order or service schedule.

Relationship to customer agreements

The applicable agreement and Ordering Document define the service actually purchased. The Cloud Service Description and service schedule identify the subscribed service scope, environments, regions, support profile, availability objectives and other service-specific terms. The Data Processing Addendum and Trust Centre policies govern data-protection and operational-control topics to the extent incorporated into the customer relationship.

3. Definitions and policy hierarchy

Term	Meaning
Cloud Service	A PCL One-managed hosted software service identified in an applicable Order or Cloud Service Description.
Production Service	The in-scope live environment used for contracted production processing.
Service Region	The approved geographic hosting or processing region identified for the subscribed service where a regional commitment applies.
Scheduled Maintenance	Planned service work that may affect availability and is handled under the applicable maintenance and SLA rules.
Unplanned Downtime	An unplanned period in which the in-scope production service is unavailable under the applicable SLA measurement rules.
Customer Data	Data submitted to, stored in or processed by the contracted PCL One service on the Customer's behalf.
Severity 1	A production-critical incident classification used for the highest-impact service conditions under the managed support model.

Document hierarchy

Document	Primary purpose
Cloud Services Agreement	Master legal and commercial framework.
Ordering Document	Purchased services, quantities, term, fees and customer-specific selections.
Cloud Service Description / Service Schedule	Service scope, environments, regions, service boundaries and service-specific objectives.
Data Processing Addendum	Processing roles, data-protection obligations and processing terms.

Document	Primary purpose
Cloud Hosting & Delivery Policy	Public baseline hosting and service-delivery practices.
Trust Centre policies	Detailed public baseline controls for resilience, retention, subprocessors, privileged access and incident notification.

4. Cloud security and administrative access

PCL One applies security controls designed to support the confidentiality, integrity and availability of Customer Data and PCL One-managed Cloud Services. Detailed security architecture and control evidence are not necessarily public and may be provided through controlled due diligence where appropriate.

Control area	Baseline treatment
Identity and privileged access	Administrative access uses named identities, strong authentication, least privilege, approval, logging and time-bound elevation. Multi-factor authentication is required for administrative access.
Emergency access	Break-glass or emergency access is treated as an exceptional path. Where supported, emergency access is disabled by default, time-boxed, logged and subject to post-use review.
Customer-data access	Support personnel access Customer Data only where necessary to provide the contracted service, troubleshoot an issue, perform approved maintenance or respond to a security event.
Logging and review	Administrative activity and material security events are logged and may be used for investigation, operational review and assurance evidence.
Security incident response	PCL One validates, contains, investigates, notifies, recovers and tracks corrective actions for material incidents in accordance with the Security Incident & Breach Notification Policy.
Provider access	Approved service providers with access are subject to contractual confidentiality, security and minimum-necessary access controls appropriate to their role.

Customer-specific access approval, network restrictions, support windows, residency restrictions or additional regulatory controls are documented in the applicable service design or service schedule where agreed.

5. Hosting, data location and service providers

PCL One may use approved cloud infrastructure, database, networking, monitoring, support and other service providers to deliver the subscribed architecture. Provider applicability varies by product, architecture, geography and enabled features. The public Subprocessor & Third-Party Services Policy identifies providers that may support PCL One services; the customer-specific schedule identifies providers actually applicable to a subscribed service where required.

Topic	Baseline position
Hosting architecture	The applicable service design identifies the PCL One-managed hosting architecture and material service-provider dependencies for the subscribed service.
Data location	Where a contractual data-residency requirement applies, the approved residency model is documented in the Order, service schedule or customer-specific data-protection terms.
Redundancy and recovery	PCL One may use geographically separate capability within the approved residency model for redundancy, backup or recovery where consistent with the subscribed architecture.
Provider governance	Security, privacy, confidentiality and service-dependency risks are assessed before a material provider is used for customer processing; written contractual safeguards are applied appropriate to the provider's role.
Provider changes	Material subprocessor changes are handled in accordance with the governing contract and the Subprocessor & Third-Party Services Policy.

CANADA-ONLY MUNICIPAL DEPLOYMENTS

Where the applicable Order adopts the Canada-only municipal residency model, production Customer Data, backups and recovery copies remain within the approved Canadian residency model, subject to the documented service architecture and any approved customer-specific exception.

6. Continuity, backup and recovery

PCL One maintains resilience, backup and recovery controls for in-scope PCL One-managed production services. Recovery objectives apply to declared service-recovery scenarios and do not represent a promise that every support case, configuration issue or unrelated dependency failure will be resolved within the same period.

Control	Baseline treatment
Backup	Automated, encrypted backups with access controls and recovery mechanisms appropriate to the subscribed service.
Backup retention	Backup cycles are documented for the subscribed service and are distinct from business-record retention schedules; backup cycles are not used to create indefinite record retention.
Restore validation	Restore testing is performed periodically to validate recoverability rather than relying only on successful backup creation.
Recovery procedures	Documented recovery runbooks and controlled restoration or failover procedures are maintained for applicable PCL One-managed components.
Recovery exercises	Periodic restore testing and at least annual disaster-recovery or recovery exercises are performed for the in-scope municipal resilience baseline, with measured outcomes and corrective actions tracked where appropriate.

Service-specific storage regions, backup frequency, recovery windows and retention periods are documented in the applicable service schedule or technical design where required.

7. Service availability and monitoring

Availability objectives apply to the in-scope production service and are measured under the applicable SLA and service-schedule rules. Scheduled maintenance, customer-caused outages and external dependencies may be excluded where the applicable SLA provides for those exclusions.

CANADIAN MUNICIPAL BASELINE

99.9% monthly production availability | RTO 4 hours | RPO 1 hour | Severity 1 acknowledgement target 15 minutes, 24x7

Measure	Baseline objective	Application
Monthly production availability	99.9%	Measured under the applicable SLA and service-schedule rules where this baseline is adopted.
Recovery Time Objective (RTO)	4 hours	Target elapsed time to restore the in-scope production service following a declared disaster or major recovery event.
Recovery Point Objective (RPO)	1 hour	Maximum targeted data-loss window for the production service following a declared recovery event.
Severity 1 acknowledgement	15 minutes, 24x7	Target acknowledgement for a production-critical incident under the managed support model.

Operational monitoring

PCL One monitors PCL One-managed service components appropriate to the subscribed architecture. Monitoring may include service health, integrations, queues, certificates, backup outcomes, platform events and security events. Monitoring coverage and customer-facing reporting may vary by service design.

Monitoring area	Purpose
Service health	Identify availability, performance or component-health conditions requiring operational attention.
Integrations and queues	Identify failed, delayed or abnormal processing conditions within PCL One-managed integration paths.
Certificates and dependencies	Identify expiring or unhealthy PCL One-managed technical dependencies where monitored.
Backup outcomes	Identify backup failures or exceptions requiring operational follow-up.

Monitoring area	Purpose
Security events	Identify relevant security events and route material findings into the incident-management process.

8. Change management and maintenance

PCL One uses controlled change and maintenance practices for PCL One-managed service components. Changes are planned, assessed and implemented according to the service architecture, operational risk and applicable customer commitments.

Change category	Baseline handling
Planned maintenance	Planned service work is scheduled and communicated in accordance with the applicable service schedule and maintenance rules. Where practicable, PCL One seeks to reduce customer impact.
Security maintenance	Urgent or critical security work may require expedited implementation when delay would create material security or service risk.
Configuration change	Customer-specific configuration changes are controlled through the agreed service-management or implementation process and may require customer approval.
Infrastructure or provider change	Material architecture or provider changes are assessed for security, privacy, residency and service-dependency impact before production use.
Service evolution	Product and service changes may be introduced as part of normal service operation. Customer-specific contractual commitments continue to be governed by the applicable Order and service terms.

Where a customer agreement or service schedule establishes a specific maintenance window, notice period, blackout period or approval process, that requirement applies to the relevant service.

9. Support and incident handling

PCL One coordinates customer support through the applicable support model and acts as the customer-facing escalation point for PCL One-managed service components and approved service-provider dependencies within the contracted service. Support channels, hours and commercial response commitments are governed by the applicable support terms and service schedule.

Support topic	Public baseline
Severity 1	Production-critical incident classification for the highest-impact service conditions. Target acknowledgement: 15 minutes, 24x7 where the Canadian municipal baseline is adopted.
Severity 2-4	Definitions and response commitments are governed by the applicable Cloud Support Policy, Order or Support Service Schedule. This policy does not create a universal public response-time commitment for Severity 2-4.
Escalation	Customers should follow the agreed support and incident-escalation process and maintain current service, security and privacy contacts.
Provider incidents	Where an underlying hosting or subprocessor incident is involved, PCL One coordinates the provider response and remains the customer-facing escalation point for the contracted service.

Security incident notification

PCL One follows the Security Incident & Breach Notification Policy for customer-facing security notifications. A confirmed breach affecting Customer Data has a baseline customer notification commitment within 12 hours of confirmation. A material customer-impacting incident has a baseline target of notification without undue delay and within 24 hours of confirmation of material customer impact. A shorter legal, regulatory or contract-specific requirement prevails where applicable.

10. Suspension, termination and service exit

Suspension and termination rights are governed by the applicable Cloud Services Agreement and Order. Operational suspension may be used only where permitted by the governing agreement, including where necessary to address material security, legal, misuse or service-integrity risk.

End-of-service data handling

The Customer retains ownership of Customer Data and may use supported export mechanisms during the service term. At termination or expiry, PCL One provides the agreed export and transition period defined by the applicable service terms. After the transition period, remaining Customer Data is securely deleted or rendered inaccessible, subject to legal retention requirements and documented backup-cycle limitations.

Where requested or contractually required, PCL One may provide a secure-data-destruction certificate identifying the scope and completion date of disposal. Residual backup copies expire through the documented backup rotation unless a legal retention obligation applies.

11. Customer responsibilities

- Maintain customer-managed identity providers, networks, endpoints, integrations, credentials and other dependencies identified in the service design.
- Maintain current technical, service, security and privacy contacts and participate in incident, recovery or maintenance coordination where customer action is required.
- Use supported access methods, protect customer-managed credentials and apply appropriate access controls to Customer users and administrators.
- Provide accurate service configuration, integration, data-classification, retention and residency requirements before production configuration is finalized.
- Complete required testing, acceptance and data-export activities within agreed project or transition windows.
- Follow the agreed support and escalation process so incidents can be classified and acted on promptly.

12. Exceptions, assurance and evidence

Exceptions and exclusions

- Availability, RTO and RPO do not automatically extend to customer-managed systems, unsupported integrations or unrelated third-party services.
- Actual recovery sequencing may depend on safety, data-integrity and security validation before production service is restored.
- Detailed architecture, system configurations, account identifiers, privileged-access design and sensitive security evidence are not disclosed in this public policy.
- Service-specific objectives, maintenance rules, support commitments, credits or remedies are governed by the applicable customer agreement, Order, service schedule and SLA.
- Legal holds, regulator instructions or active investigations may delay routine deletion or limit the content or timing of certain disclosures where legally required.

Assurance and evidence

PCL One maintains records supporting the operation of this policy. Detailed evidence may be provided to eligible customers, prospective customers, business partners or regulators through controlled due diligence, subject to applicable report-use and confidentiality restrictions.

- Service availability and incident records.
- Backup success, restore-test and recovery-exercise records.
- Administrative-access, MFA and privileged-access evidence.
- Change, maintenance and operational-event records where applicable.
- Customer notification, root-cause and corrective-action records for material incidents.
- Provider due-diligence and material-change records.

PCL One maintains a SOC 2 Type 2 report covering controls relevant to Security, Confidentiality and Availability within the scope of that report. The full report is restricted-use assurance evidence and is not incorporated into this public policy by publication.

13. Statement of changes

Effective date	Summary
6 October 2025	Initial publication of this policy.