



CONTRACTS & POLICIES

PCL One Cloud Service Description



STANDARD SERVICE SCOPE, DELIVERY MODEL AND SERVICE BOUNDARIES

Effective Date: 6 October 2025

Classification: Public

Document ID: PCL-CONTRACT-SERVICE-019

This document describes the baseline scope and delivery model for PCL One-managed Cloud Services. The applicable Ordering Document identifies the specific services, modules, quantities, environments, regions, support profile and customer-specific commitments purchased by a Customer.

Contents

This Service Description should be read together with the applicable PCL One Cloud Services Agreement, Ordering Document, Data Processing Addendum, Cloud Support Policy and referenced Trust Centre policies.

01	Overview
02	Scope and applicability
03	Service components and service boundaries
04	Deployment model and environments
05	Customer data, configuration and integrations
06	Hosting, data residency and service providers
07	Availability, resilience and backup
08	Support and incident management
09	Security and privileged access
10	Change, maintenance and release management
11	Data lifecycle, export and contract exit
12	Customer responsibilities
13	Service-specific schedules and precedence
14	Assurance and evidence
15	Statement of changes

POLICY STATUS

This is a public baseline Service Description. The specific Cloud Services purchased by a Customer, together with any customer-specific service levels, regions, quantities, exclusions or enhanced commitments, are governed by the applicable Cloud Services Agreement, Ordering Document and Service Schedule.

1. Overview

PCL One provides managed cloud software and related service capabilities for business, public-sector and regulated-customer use cases. This Service Description establishes the baseline delivery model for PCL One-managed Cloud Services and explains how service scope, environments, hosting, resilience, support, security, change management and contract exit are applied.

A Customer purchases only the services and entitlements identified in its Ordering Document. General product capability, roadmap content, demonstrations, proposal descriptions or publicly available information do not expand the subscribed service unless expressly included in the applicable Order or Service Schedule.

2. Scope and applicability

This Service Description applies to PCL One-managed Cloud Services where it is incorporated by reference into the applicable Agreement, Order or Service Schedule. It covers the PCL One-managed service boundary, operational responsibilities, service environments, hosting and provider dependencies, support interfaces, data lifecycle and supporting assurance evidence.

Implementation services, data conversion, consulting, custom development, third-party licenses and customer-managed infrastructure are included only where expressly stated in an Order, Statement of Work or Service Schedule.

RELATIONSHIP TO CUSTOMER AGREEMENTS

If the applicable Agreement, Order, Service Schedule, Data Processing Addendum or customer-specific security terms contain a more specific or stricter commitment for a subscribed service, that customer-specific commitment governs to the extent of conflict.

3. Service components and service boundaries

Service component	Baseline treatment	Contract-specific source
Application service	PCL One operates the subscribed application capabilities identified in the Order and makes them available to authorized users through the supported service interface.	Ordering Document / Service Schedule
Managed platform components	PCL One manages the service components assigned to PCL One within the approved technical design, including applicable application, database, integration, monitoring and operational components.	Service design / Service Schedule
Hosting and infrastructure	Hosting is provided through PCL One-managed infrastructure or approved cloud/service providers selected for the subscribed architecture.	Order / Subprocessor Policy
Monitoring and operations	PCL One monitors service health and PCL One-managed components using operational and security monitoring appropriate to the service.	Service Resilience & Recovery Policy
Backup and recovery	Backups and recovery controls are applied according to the service-specific recovery design and documented recovery window.	Service Schedule / Data Retention Policy
Support	Support is delivered under the applicable support profile, severity model and escalation process.	Cloud Support Policy / Service Schedule
Security administration	PCL One applies administrative-access controls, logging, strong authentication and privileged-access governance to PCL One-managed environments.	Privileged Support & Emergency Access Policy

Service boundary exclusions

Unless expressly included in the applicable Order or Service Schedule, the baseline Cloud Service does not include:

- Customer-owned networks, internet connectivity, endpoints, printers, mobile devices, local infrastructure or physical facilities.
- Administration of the Customer's identity provider, directory, endpoint-security platform or customer-managed credentials.
- Third-party applications, interfaces or services that are not identified as PCL One-managed dependencies in the subscribed service design.
- Customer-specific data cleansing, historical-data remediation, business-process redesign, implementation consulting or custom development.
- Premium support, non-standard support hours, enhanced recovery objectives, non-standard retention, special residency requirements or dedicated infrastructure unless purchased.
- Legal, records-management, privacy-notice or regulatory decisions that remain the Customer's responsibility.

4. Deployment model and environments

The deployment model for each Customer is defined in the applicable Order and service design. PCL One may provide production and non-production environments according to the subscribed service. Separate development, test, training, sandbox or reporting environments are included only where identified in the applicable Order or Service Schedule.

Environment	Purpose	Baseline position
Production	Live processing of the subscribed business service.	Subject to the applicable availability, support, backup and recovery commitments.
Test / sandbox	Configuration validation, integration testing, release testing or user acceptance activities.	Included only where ordered; may have different availability, backup and support treatment from production.
Development / configuration	Controlled configuration or technical development activities.	Included only where the architecture and Order provide for a separate environment.
Training	Training, demonstration or practice activity using approved data.	Included only where ordered; production personal data should not be copied unless approved and protected.

Non-production environments are not treated as production unless the applicable Order expressly states otherwise. Customer acceptance, testing and release-readiness activities may be performed in non-production environments before changes are promoted to production.

5. Customer data, configuration and integrations

Customer Data remains subject to the ownership and use provisions of the Cloud Services Agreement and applicable data-protection terms. The Customer controls the business content submitted to the service and is responsible for the accuracy, lawfulness, classification and permitted use of that data.

Configuration

PCL One Cloud Services may include configurable workflows, roles, forms, rules, notifications, reporting, retention settings and integration parameters. Configuration is applied within the supported service model. Customer-specific extensions, bespoke code or unsupported modifications are included only where expressly agreed.

Integrations

Interfaces with customer-managed or third-party systems are governed by the applicable service design. PCL One is responsible for PCL One-managed integration components identified in that design; the Customer remains responsible for the availability, credentials, security and operation of customer-managed endpoints and third-party systems unless the applicable Order states otherwise.

Integration responsibility	PCL One baseline	Customer baseline
Interface configuration	Configure and operate PCL One-managed integration components included in the subscribed scope.	Provide accurate endpoint details, credentials, certificates, data mappings and business rules.
Connectivity	Operate PCL One-managed network and service components.	Maintain customer networks, firewalls, allow-lists, identity services and endpoints required for connectivity.
Data quality	Apply agreed service validation and processing controls.	Provide complete, accurate and authorized source data and resolve source-system data defects.

Integration responsibility	PCL One baseline	Customer baseline
Third-party changes	Coordinate changes to PCL One-managed dependencies where applicable.	Notify PCL One of customer or third-party changes that may affect integrations.

6. Hosting, data residency and service providers

PCL One uses approved hosting, infrastructure, database, support and other service providers where required 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 the subscribed service where required.

The applicable Order or Service Schedule identifies the approved production data-residency model where a contractual residency requirement applies. PCL One may use geographically separate locations within the approved residency model for redundancy, backup or recovery where consistent with the contracted service design.

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.

7. Availability, resilience and backup

Availability and recovery objectives apply only to the in-scope production service and are measured under the applicable Service Schedule and SLA rules. They do not convert every support case, configuration issue, customer-managed dependency failure or third-party integration issue into a disaster-recovery event.

Measure	Public baseline where adopted	Application
Monthly production availability	99.9%	Applies where the Order or Service Schedule adopts the PCL One Canadian municipal baseline.
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 in-scope 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.

Where an Order establishes different objectives, measurement rules, exclusions, support commitments or service-credit terms, the Order and applicable SLA govern for that Customer.

Backup and recovery controls

- Automated backups with encryption and role-controlled administrative access appropriate to the subscribed service.
- Documented backup and recovery cycles that are distinct from business-record retention schedules.
- Periodic restore testing to validate recoverability rather than relying only on successful backup creation.
- Recovery runbooks and controlled restoration or failover procedures for PCL One-managed components.
- At least annual disaster-recovery or recovery exercises for the in-scope resilience baseline, with measured outcomes and tracked corrective actions where applicable.

8. Support and incident management

PCL One provides support through the channels and service hours identified in the applicable Cloud Support Policy and Service Schedule. Severity classification is based on business and service impact. The public baseline publishes a timed acknowledgement target for Severity 1; customer-specific targets for other severity levels are governed by the applicable support profile and Order.

Severity	Public description	Response commitment
Severity 1 - Critical	Production-critical condition causing the highest level of business or service impact, such as material unavailability of	15-minute acknowledgement target, 24x7, where the applicable baseline is adopted.

Severity	Public description	Response commitment
	the in-scope production service.	
Severity 2 - Significant	Significant impairment of important functionality where production remains available but business operation is materially affected.	As stated in the applicable Support Service Schedule or Order.
Severity 3 - Technical	Technical issue with limited business impact, workaround availability or non-critical functional impairment.	As stated in the applicable Support Service Schedule or Order.
Severity 4 - Guidance	General question, information request, configuration guidance or low-impact service request.	As stated in the applicable Support Service Schedule or Order.

Security incidents and confirmed breaches are handled under the Security Incident & Breach Notification Policy. Customer communications are directed to the designated security, privacy and service contacts recorded for the engagement.

9. Security and privileged access

PCL One applies security controls designed to protect the confidentiality, integrity and availability of Customer Data and the in-scope service. Detailed security architecture and assurance evidence may be provided through controlled due diligence where appropriate.

Control area	Baseline approach
Identity and administrative access	Named identities, strong authentication, least privilege and role-controlled access are used for PCL One administrative activity.
Privileged elevation	Privileged access is activated for an approved service need and is time-bound where the service architecture supports that model.
Logging and review	Administrative and security-relevant activity is logged. Material or emergency access is reviewable and may form part of assurance evidence.
Emergency access	Break-glass or equivalent recovery access is treated as an exceptional path and is controlled, logged and reviewed.
Data access	PCL One personnel access Customer Data only where necessary to provide the contracted service, troubleshoot an issue, perform approved maintenance or respond to a security event.
Provider access	Approved service providers with support access are subject to appropriate confidentiality, minimum-necessary and security controls for their role.

10. Change, maintenance and release management

PCL One maintains controlled processes for service changes, maintenance and security updates. The timing and notice requirements for planned maintenance, material customer-impacting changes and customer testing are governed by the applicable Service Schedule or support terms.

Baseline change principles

- Changes are assessed for service, security, privacy and dependency impact before production deployment where appropriate.
- Material changes affecting customer configuration, integrations, processing location or provider use are coordinated under the applicable contractual process.
- Security or emergency maintenance may be performed on an expedited basis when required to protect the service or Customer Data.
- Customer testing or acceptance may be required where a change materially affects customer-managed integrations, workflows or configurations.
- Public documentation may be updated to reflect service evolution; an executed Order continues to govern customer-specific commitments for the applicable service period.

11. Data lifecycle, export and contract exit

Data retention, backup and secure disposal are governed by the Data Retention, Backup & Secure Disposal Policy and any customer-specific retention schedule. PCL One does not impose one universal business-record retention period across data categories where legal or operational requirements differ.

Lifecycle stage	Baseline treatment
Active service	Customer Data is processed for the subscribed service and retained according to the configured or contracted records schedule.
Legal or operational hold	Routine deletion is suspended only for affected data where a documented hold, investigation, records-freeze or statutory requirement applies.
Export / transition	The Customer may use supported export mechanisms during the service term and an agreed transition window at termination or expiry.
Production disposal	After the agreed transition period, remaining production Customer Data is deleted or rendered inaccessible, subject to legal retention requirements.
Residual backups	Backup copies expire through the documented backup cycle unless continued preservation is legally required.
Destruction confirmation	Where requested or contractually required, PCL One may provide a secure-data-destruction confirmation identifying the applicable scope and completion date.

12. Customer responsibilities

The Customer is responsible for the controls and decisions that remain within the Customer environment or business process. These responsibilities include, as applicable:

- Maintaining authorized users, customer-side role assignments, designated approvers and current security, privacy, billing and service contacts.
- Protecting customer-managed administrator accounts, identity systems, credentials, endpoints, networks and integration components.
- Providing lawful, accurate and appropriately classified Customer Data and obtaining required notices, consents or other legal basis for processing.
- Providing and maintaining customer-managed integration endpoints, certificates, network rules and third-party dependencies identified in the service design.
- Participating in user acceptance testing, release validation, recovery coordination and incident investigation where customer action is required.
- Providing retention schedules, legal-hold instructions, residency constraints and industry or regulatory requirements that PCL One is expected to implement.
- Completing required data exports during the agreed exit period and validating exported data before final disposal.

13. Service-specific schedules and precedence

The following documents work together to define the subscribed Cloud Service. Not every document applies to every Customer or service. The executed Order identifies the applicable documents and any customer-specific variations.

Document	Primary purpose
PCL One Cloud Services Agreement	Master legal and commercial terms governing Cloud Services.
Cloud Services Ordering Document	Customer, purchased services, quantities, fees, term, environments and transaction-specific terms.
This Cloud Service Description	Baseline service scope, delivery model and service boundaries.
Cloud Support Policy / Support Service Schedule	Support channels, severity model, support hours, response targets and escalation terms.
Service Resilience & Recovery Policy / SLA	Availability, recovery objectives, measurement rules and any service-credit terms.
Data Processing Addendum	Data-protection roles, instructions, subprocessors and personal-data obligations.
Trust Centre policies	Operational baselines covering incidents, retention, subprocessors, privileged access and other published controls.
Statement of Work	Implementation, consulting, data migration, custom development or other professional services where purchased.

Where these documents conflict, the order of precedence stated in the Cloud Services Agreement and applicable Ordering Document governs. A customer-specific term does not automatically amend the public baseline for other customers.

14. Assurance and evidence

PCL One maintains records supporting the operation of the controls described in this Service Description. Detailed security evidence is not necessarily public and may be provided to eligible customers, prospective customers, business partners or regulators through controlled due diligence, subject to applicable confidentiality and report-use restrictions.

- Service architecture and approved service-design records.
- Availability, incident and service-management records.
- Backup success, restore-test and recovery-exercise evidence.
- Administrative-access, privileged-elevation and emergency-access records where applicable.
- Customer-specific subprocessor, residency and data-flow documentation where required.
- Relevant assurance reports, certifications, penetration-test summaries or other evidence where available and appropriate for disclosure.

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 Service Description by publication.

15. Statement of changes

Effective date	Summary
6 October 2025	Initial publication of this Cloud Service Description.