TRUST CENTRE

Data Retention, Backup & Secure Disposal Policy

CUSTOMER DATA LIFECYCLE, BACKUP AND CONTRACT EXIT

Effective Date: 6 October 2025

Classification: Public

This document is intended for public distribution. Supporting assurance evidence may be subject to separate access and confidentiality restrictions.

Contents

This policy should be read together with the applicable customer agreement, order, service schedule and data-protection terms.

1. Overview

This policy describes PCL One's baseline treatment of customer records, audit information, backups, migration data and end-of-service disposal. The model is designed to support records-retention obligations without imposing one universal retention period on data categories that may have different legal or operational requirements.

> **POLICY STATUS**
> This is a public baseline policy. Service-specific commitments are governed by the applicable agreement, order, service schedule and data-protection terms.

2. Scope and applicability

- Applies to customer data and associated service records held within PCL One-managed environments.
- Covers retention configuration, legal holds, backup handling, data export, transition and secure disposal.
- Service-specific storage regions, backup frequency and retention windows are documented in the applicable service schedule or technical design where required.

Relationship to customer agreements

Customer-specific retention requirements are governed by the applicable agreement, service schedule, records schedule and law. If those documents set stricter or more specific obligations than this policy, the customer-specific obligations prevail.

3. Definitions

Term	Meaning
Retention Schedule	The approved period for retaining a category of customer data before disposal, archival or review.
Legal Hold	A documented instruction that suspends routine deletion for identified data because of litigation, investigation, audit or statutory requirements.
Backup	A protected copy created to support service recovery. Backup retention is distinct from the business-record retention schedule.
Secure Disposal	Deletion, destruction or irreversible rendering-inaccessible of data in accordance with the applicable retention and backup cycle.

4. Data lifecycle policy

Data category	Baseline position	Control approach
Business records and attachments	Customer-approved schedule	Retention is configured by record category where supported. Active legal or operational holds override routine deletion.
Audit, configuration and security logs	Contracted or customer-approved schedule	Retained for audit, investigation, service and compliance purposes and made available through supported search or export mechanisms.

Data category	Baseline position	Control approach
Operational telemetry	Service-specific minimum necessary period	Collected for service operation, security and support. Unnecessary personal data should not be introduced into telemetry.
Backups	Service-specific backup cycle	Backups are automated, encrypted, access-controlled and retained for the documented recovery window. Backup cycles are not used to create indefinite record retention.
Migration and staging data	Only as long as required for migration, validation and acceptance	Removed or de-identified when no longer required, subject to legal, contractual or active-issue needs.
Data after contract end	Agreed export/transition window followed by disposal	Production data is deleted or rendered inaccessible after the agreed transition period. Residual backup copies expire through the documented backup cycle unless law requires otherwise.

Backuphandling

Backups are encrypted and protected by role-based administrative controls.

For Canada-only municipal deployments, backup and recovery copies remain within the approved Canadian residency model.

Restore testing is performed periodically to validate recoverability, not simply successful backup creation.

A customer deletion instruction is applied to the active service in accordance with the approved process; residual backup copies expire through the documented backup rotation unless a legal retention obligation applies.

End-of-serviceexportand disposal

The customer retains ownership of customer data and may use supported export mechanisms during the service term.

At termination or expiry, PCL One provides an agreed data-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 can provide a secure-data-destruction certificate identifying the scope and completion date of disposal.

Legal holds and retention exceptions

A documented legal hold, investigation hold, records-freeze instruction or statutory requirement suspends routine deletion only for the affected data. Once the hold is released, the normal retention schedule resumes. Material exceptions should have a defined reason, owner and review point.

5. Customer responsibilities

Provide or approve the retention schedule that applies to customer-controlled record categories.

Notify PCL One of legal holds or records-freeze instructions affecting data that PCL One is expected to retain.

Complete required exports during the agreed transition period and validate that exported data is usable before final disposal.

6. Exceptions and exclusions

Retention and deletion may be delayed where law, legal hold, security investigation or binding regulator instruction requires continued preservation.

Third-party repositories, customer-managed exports and data copied outside the PCL One service are governed by the controls of the receiving environment.

Backup expiration follows the documented service-specific cycle and may not be immediate at the same moment as active-record deletion.

7. Assurance and evidence

PCL One maintains records supporting the operation of this policy. 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 report-use and confidentiality restrictions.

Customer retention configuration or schedule record.

Backup success and restore-test evidence.

Legal-hold or retention-exception records where applicable.

Exit/export records and secure-disposal confirmation.

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.

8. Statement of changes

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