TRUST CENTRE

Service Resilience & Recovery Policy

BUSINESS CONTINUITY, DISASTER RECOVERY AND SERVICE OBJECTIVES

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 resilience, backup, monitoring and disaster-recovery approach for in-scope municipal cloud production services. It also explains how availability, Recovery Time Objective (RTO), Recovery Point Objective (RPO) and critical-incident acknowledgement targets are applied.

> **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 PCL One municipal cloud production services where the applicable order or service schedule adopts these baseline objectives.

Covers production availability, recovery objectives, monitoring, backup, recovery exercises and supporting operational evidence.

Does not convert every support incident or third-party dependency failure into a declared disaster-recovery event.

Relationship to customer agreements

The applicable agreement, order and service schedule define the service actually purchased and may establish different objectives, measurement rules, exclusions or service-credit terms. Where contract-specific terms differ, they govern the applicable service.

3. Definitions

Term	Meaning
Availability	The percentage of time an in-scope production service is available during the applicable measurement period, subject to the service schedule and SLA measurement rules.
RTO	Recovery Time Objective - the target elapsed time to restore an in-scope production service following a declared disaster or major recovery event.
RPO	Recovery Point Objective - the maximum targeted data-loss window measured from the point of recovery following a declared recovery event.
Severity 1	A production-critical incident classification used under the managed support model for the highest-impact service conditions.

4. Resilience and recovery commitments

> **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.
Recovery Time Objective (RTO)	4 hours	Target 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.

Resilience design baseline

Automated, encrypted backups with recovery mechanisms appropriate to the subscribed service.

For Canada-only municipal deployments, geographically separate recovery capability within the approved Canadian residency model.

Monitoring of service health, integrations, queues, certificates, backup outcomes and security events for PCL One-managed components.

Documented recovery runbooks and controlled restoration or failover procedures.

Periodic restore testing and at least annual disaster-recovery or recovery exercise with measured outcomes and tracked corrective actions.

How RTO and RPO are applied

RTO and RPO apply to a declared service-recovery scenario affecting the in-scope production platform. They are recovery objectives, not a promise that every support case, configuration issue or third-party integration problem will be resolved within the same period. Dependencies outside PCL One's control are coordinated through the incident process and documented in the service design where relevant.

5. Customer responsibilities

Maintain customer-managed dependencies identified in the service design, including identity providers, networks, integration endpoints and required credentials.

Maintain current critical contacts and participate in recovery coordination or testing where customer action is required.

Follow agreed support and incident-escalation procedures so critical events can be classified and acted on promptly.

6. Exceptions and exclusions

Scheduled maintenance, customer-caused outages and external dependencies may be excluded from availability calculations where the applicable SLA says so.

RTO and RPO apply to the in-scope service and do not automatically extend to customer-managed systems or unrelated third-party services.

Actual recovery sequencing may depend on safety, data-integrity and security validation before production service is restored.

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.

Service availability and incident reporting.

Backup success and restore-test records.

Recovery-exercise results, measured recovery outcomes and corrective actions.

Material incident and problem-management 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.

8. Statement of changes

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