TRUST CENTRE

Privileged Support & Emergency Access Policy

ADMINISTRATIVE ACCESS, TIME-BOUND ELEVATION AND BREAK-GLASS CONTROL

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 how PCL One governs administrative support access to in-scope customer environments. The baseline model avoids unrestricted standing access to customer data and uses named identities, multi-factor authentication, least privilege, approval, logging and time-bound elevation. Emergency or break-glass access is treated as an exceptional control path.

> **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 personnel and approved service providers requiring administrative access to PCL One-managed customer environments.

Covers normal support access, privileged elevation, emergency access, logging, review and customer control options.

Customer-specific access approval, network restrictions and residency requirements are documented in the applicable service design or schedule.

Relationship to customer agreements

The applicable agreement and service design define the access model for the subscribed service. Customer-specific restrictions, approval requirements or regulatory controls that are expressly agreed take precedence for the applicable environment.

3. Definitions

Term	Meaning
Privileged Access	Administrative access capable of changing configuration, managing security-relevant settings or accessing data beyond ordinary end-user permissions.
Time-Bound Elevation	Temporary activation of privileged permissions for a defined task and period, with removal or expiry when the task is complete.
Break-Glass Access	An emergency access path used when normal administrative access cannot safely support recovery or response.
Named Account	An identity uniquely attributable to an authorized individual rather than a shared generic administrator credential.

4. Privileged access controls

Stage	Baseline control
1. Need established	A support case, approved maintenance task, security event or other documented service need establishes the purpose for access.
2. Authorization	Access is approved under the engagement's support and security model. Customer approval is used where the service schedule requires case-by-case authorization.

Stage	Baseline control
3. Least privilege	Only the role, environment and data scope necessary for the task are granted. Named administrator accounts are used.
4. Strong authentication	Multi-factor authentication is required for administrative access. Federated access may use the customer or PCL One identity provider according to the agreed design.
5. Time-bound elevation	Privileged access is activated only for the required window and removed or expires when the task is complete.
6. Logging and review	Administrative activity is logged. Material or emergency access is reviewable and may be included in assurance evidence where appropriate.

Emergency / break-glass access

Break-glass or emergency access accounts are disabled by default wherever the architecture supports that model.

Activation is reserved for conditions such as federated sign-on failure, a critical service-recovery event or another situation where normal administrative access cannot safely restore or secure the service.

Activation requires dual authorization, is time-boxed, and each use is logged and reviewed after the event.

Emergency access does not remove the requirements for least privilege, evidence preservation or applicable customer incident communication.

Customer data and geography

Support personnel access customer data only when necessary to provide the contracted service, troubleshoot an issue, perform approved maintenance or respond to a security event.

Remote support access does not by itself relocate the stored customer dataset. For a Canada-only municipal deployment, customer data, backups and recovery copies remain within the approved Canadian residency model.

Processing outside the approved residency model requires the disclosure and customer approval or contract treatment specified for the engagement.

Approved subprocessors with support access are subject to equivalent minimum-necessary, confidentiality and security controls appropriate to their role.

Customer control options

Named customer approvers for privileged support access.

Case-by-case approval for data-level access where operationally feasible and agreed.

IP or network restrictions, support windows or additional access conditions where supported by the service architecture.

Periodic administrative-access review and assurance reporting where agreed for the service.

5. Customer responsibilities

Maintain designated approvers and escalation contacts where customer approval is part of the access model.

Protect customer-managed administrator identities and promptly notify PCL One of access changes that affect support or service operation.

Avoid sharing privileged credentials outside the agreed identity and access-management process.

6. Exceptions and exclusions

Emergency access may be unavailable in architectures that do not support a separate disabled-by-default break-glass identity; equivalent controlled recovery mechanisms are used where applicable.

Customer-managed identity, network or endpoint failures may require coordinated action before PCL One support access can be established.

Detailed privileged-access configurations, account identifiers and security architecture are not disclosed in this public policy.

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.

Named privileged-account inventory.

MFA and identity-configuration evidence.

Privileged-access grant and expiry records.

Administrative and audit-log extracts.

Break-glass activation and post-use review records where applicable.

Periodic access-certification results where performed.

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.