



TRUST CENTRE

Cloud Support Policy



SUPPORT REQUESTS, SEVERITY CLASSIFICATION, RESPONSE AND ESCALATION

Effective Date: 6 October 2025

Classification: Public

Document ID: PCL-TRUST-SUP-018

This document is intended for public distribution. Customer-specific support entitlements, response commitments, escalation contacts, support hours and commercial remedies may be governed by the applicable agreement, Ordering Document or Support Service Schedule.

Contents

This policy should be read together with the applicable Cloud Services Agreement, Ordering Document, Cloud Service Description, Cloud Hosting & Delivery Policy, Service Resilience & Recovery Policy, Security Incident & Breach Notification Policy and customer-specific support terms.

01	Overview
02	Scope and applicability
03	Definitions
04	Support access and customer contacts
05	Severity classification
06	Severity 1 response target
07	Severity 2-4 customer-specific commitments
08	Service request lifecycle and communications
09	Escalation and incident coordination
10	Support access and security
11	Maintenance, updates and exclusions
12	Customer responsibilities
13	Assurance and evidence
14	Statement of changes

1. Overview

This policy describes PCL One's public baseline for customer support of in-scope cloud services. It explains how support requests are received, classified, acknowledged, coordinated, escalated and closed. The policy is designed to make Severity 1 handling transparent while preserving customer-specific commercial terms for lower-severity support conditions.

POLICY STATUS

This is a public baseline policy. The Severity 1 acknowledgement target stated here is a public support objective. Response targets for Severity 2 through Severity 4, service hours, update frequencies, remedies and premium support entitlements are governed by the applicable agreement, Ordering Document or Support Service Schedule.

2. Scope and applicability

This policy applies to PCL One-managed cloud production services and support operations where PCL One is responsible for customer-facing support. It covers support intake, severity classification, acknowledgement, technical coordination, customer communications, escalation and closure.

This policy does not convert implementation work, configuration changes, enhancement requests, training, professional services or unrelated third-party issues into support incidents unless those activities are expressly included in the subscribed support service.

Relationship to customer agreements

The applicable Cloud Services Agreement, Ordering Document, Cloud Service Description and Support Service Schedule define the service actually purchased. Where customer-specific terms establish different support hours, response commitments, escalation processes or remedies, those terms govern the relevant service to the extent of conflict.

3. Definitions

Term	Meaning
Acknowledgement	Confirmation that PCL One has received a support request, assigned or validated its severity and initiated the applicable support workflow. Acknowledgement is not a commitment to resolution within the same period.
Service Request	A customer support case or request submitted through an approved support channel for an in-scope service.
Production Service	The customer-facing production environment identified in the applicable Order or Cloud Service Description.
Workaround	A temporary measure that materially restores or preserves business operation while the underlying issue is investigated or corrected.
Resolution	A correction, recovery action, configuration change, documented workaround or other action that addresses the support condition to the extent required under the applicable support terms.
Business Hours	The support hours defined in the applicable Order or Support Service Schedule for non-24x7 support activities.

4. Support access and customer contacts

Customers submit support requests through the approved channels communicated for the engagement. Depending on the subscribed service, approved channels may include a support portal, support email, telephone escalation or other designated service-management channel.

Support requirement	Baseline position
Authorized contacts	The Customer maintains current technical and business contacts authorized to open, update and escalate support requests.
Critical contacts	The Customer maintains reachable contacts for Severity 1 coordination, including after-hours contacts where 24x7 support applies.
Case information	Support requests should include the affected service, environment, business impact, start time, users or functions affected, recent changes and relevant evidence reasonably available.

Support requirement	Baseline position
Secure information exchange	Sensitive credentials, personal data, logs or evidence should be exchanged only through approved secure channels and only to the extent reasonably necessary for support.
Case ownership	PCL One assigns support ownership appropriate to the request and coordinates PCL One-managed dependencies and approved service providers where relevant.

5. Severity classification

Severity is based primarily on the business and production impact of the support condition, not solely on the urgency assigned by the requester. The Customer may propose an initial severity when opening a case. PCL One may validate or adjust the severity to align with the definitions below and will communicate a material reclassification through the support case or agreed contact channel.

Severity	Public definition	Typical indicators
Severity 1 - Critical	A production-critical condition causing the in-scope production service, or a critical business function within it, to be unavailable or materially unusable with no reasonable workaround.	Widespread production outage; critical payroll or other time-sensitive production processing stopped; material service-integrity condition requiring immediate action.
Severity 2 - Significant	A significant production impairment that materially affects an important function or substantial group of users, but the service remains partly usable or a reasonable workaround exists.	Important function unavailable or severely degraded; substantial operational disruption; workaround available but materially burdensome.
Severity 3 - Technical	A limited-impact technical issue where core production operations can continue and a reasonable workaround or alternative path is available.	Non-critical defect; isolated function or user impact; intermittent issue with limited business effect.
Severity 4 - Guidance	A request for information, guidance, clarification or other non-incident assistance that does not materially impair production operation.	How-to question; documentation clarification; general service inquiry; non-urgent administrative request.

SEVERITY PRINCIPLE

Severity 1 is reserved for production-critical conditions. Non-production issues, feature requests, project tasks, planned maintenance, training requests and isolated user questions are not normally Severity 1 unless they cause a qualifying critical production impact.

6. Severity 1 response target

PUBLIC SEVERITY 1 BASELINE

PCL One targets acknowledgement of a valid Severity 1 support request within 15 minutes, 24x7, for an in-scope production service. This is an acknowledgement target, not a guaranteed resolution time.

For an accepted Severity 1 condition, PCL One initiates critical-incident handling appropriate to the affected service. Activities may include validating impact, assigning accountable technical ownership, engaging relevant operations or service-provider teams, establishing a customer communication channel, preserving evidence where required and working toward service restoration or a safe workaround.

Severity 1 handling element	Baseline approach
Coverage	24x7 for valid Severity 1 support requests affecting an in-scope production service.
Acknowledgement target	15 minutes from receipt through an approved critical-support channel, subject to the request containing sufficient information to identify the customer and affected service.
Technical ownership	An accountable support or operations owner is assigned and relevant technical resources are engaged according to the incident.
Customer coordination	PCL One coordinates with the designated customer contact and requests customer actions or information where required to investigate or restore service.
Updates	Status updates are provided through the agreed incident channel at intervals appropriate to the incident and any customer-specific support terms.

Severity 1 handling element	Baseline approach
Restoration and follow-through	Priority is placed on safe restoration or a workable mitigation. Root-cause and corrective-action follow-through is performed where appropriate to the materiality of the incident.

The Severity 1 acknowledgement target may depend on the Customer using the approved critical-support route and maintaining reachable critical contacts. Delays caused by inaccessible customer-managed systems, unavailable customer contacts or missing information may affect investigation and restoration activities but do not change the classification principles in this policy.

7. Severity 2-4 customer-specific commitments

PCL One publishes the definitions of Severity 2, Severity 3 and Severity 4 so customers can classify support needs consistently. PCL One does not establish universal public response-time commitments for Severity 2 through Severity 4 in this policy.

Severity	Public website position	Contractual treatment
Severity 2	Definition published; no universal public response target.	Response hours and acknowledgement targets are defined in the applicable Order or Support Service Schedule.
Severity 3	Definition published; no universal public response target.	Response hours and acknowledgement targets are defined in the applicable Order or Support Service Schedule.
Severity 4	Definition published; no universal public response target.	Response hours and acknowledgement targets are defined in the applicable Order or Support Service Schedule.

Customer-specific support plans may provide different coverage windows, named resources, priority queues, update frequencies or other service levels. Those commitments apply only where expressly included in the applicable Order or Support Service Schedule.

8. Service request lifecycle and communications

Stage	Baseline control
1. Intake	Receive the support request through an approved channel and associate it with the applicable customer and service.
2. Validate and classify	Confirm the reported impact, validate severity, identify the affected environment and determine whether the condition is within the subscribed support scope.
3. Assign ownership	Assign an accountable support owner and engage operations, engineering or approved service providers as required.
4. Investigate and mitigate	Collect relevant evidence, test hypotheses, identify a workaround or corrective action and coordinate customer-side actions where necessary.
5. Communicate	Provide material status information through the agreed support channel and identify any customer action, decision or next update point that is reasonably required.
6. Restore or resolve	Restore service, implement an appropriate correction or confirm a supported workaround consistent with the applicable support terms.
7. Close and improve	Confirm closure, document relevant findings and track corrective or problem-management actions where the issue is material or recurring.

Case communications

Support communications are directed to the contacts recorded for the engagement. PCL One may request logs, timestamps, screenshots, sample records, configuration information or temporary diagnostic access where reasonably necessary. Customers should avoid sending credentials or unnecessary personal data in ordinary support messages.

A support case may be placed in a waiting-for-customer state when progress requires customer information, access, approval or testing. The applicable support terms may define how such periods affect response or resolution measurements.

9. Escalation and incident coordination

A customer may request escalation when business impact materially increases, a case is not progressing as expected, or additional management or technical coordination is reasonably required. Escalation does not automatically change the case severity; severity continues to be determined by the production impact definitions in this policy.

Escalation type	Purpose
Technical escalation	Engage additional technical expertise or a higher support tier for investigation or remediation.
Operational escalation	Engage service operations, hosting or approved service-provider teams for platform or dependency coordination.
Management escalation	Engage service-management leadership where prioritization, coordination or customer communication requires additional oversight.
Security incident coordination	Route qualifying security events into the Security Incident & Breach Notification Policy while maintaining customer-facing support coordination.
Problem management	Review recurring or material incidents for root cause, trend analysis and corrective actions where appropriate.

Where an underlying hosting provider, subprocessor or other approved service provider is involved, PCL One coordinates the provider response and remains the customer-facing escalation point for the contracted PCL One service, subject to the responsibilities and limitations in the applicable service terms.

10. Support access and security

PCL One support personnel access customer environments and Customer Data only to the extent reasonably necessary to provide the contracted service, troubleshoot an issue, perform approved maintenance or respond to a security or service event. Administrative support access is governed by the Privileged Support & Emergency Access Policy.

Control	Baseline
Named identities	Administrative access uses identities attributable to authorized individuals rather than shared generic support credentials where the architecture supports named identity.
Strong authentication	Multi-factor authentication is required for administrative access to PCL One-managed customer environments.
Least privilege	Support access is limited to the role, environment and data scope reasonably necessary for the support task.
Time-bound elevation	Privileged permissions are activated for the required support window and removed or expire when the task is complete where supported by the architecture.
Logging and review	Administrative activity is logged. Material or emergency access is reviewable and may be included in assurance evidence where appropriate.
Emergency access	Break-glass or equivalent recovery access is controlled, limited to qualifying conditions and subject to post-use review where applicable.

11. Maintenance, updates and exclusions

Maintenance and service changes

Planned maintenance, software updates and service changes are governed by the Cloud Hosting & Delivery Policy and the applicable service schedule. Planned maintenance or customer-approved change activity is not treated as an unplanned support incident solely because service access is intentionally limited during the approved change window.

Support scope exclusions

- Customer-managed networks, identity providers, endpoints, devices, credentials or other systems outside PCL One's contracted management scope, except to the extent support coordination is expressly included.
- Unsupported third-party software, integrations or modifications not approved as part of the subscribed service design.
- Training, implementation, data migration, report development, configuration projects, custom development or enhancement requests unless separately ordered or included in the support plan.
- Issues caused by use outside published documentation, agreed configuration, licensed capacity or supported technical requirements where such use is the material cause of the condition.

- Security testing, load testing or other activities that may affect production service unless authorized and coordinated in advance.

PCL One will coordinate in good faith where an issue crosses customer-managed or third-party boundaries. Responsibility, service levels and remedies remain subject to the governing agreement and service design.

12. Customer responsibilities

- Use the approved support channels and identify the affected customer, service and environment when opening a support request.
- Provide an accurate description of business impact and avoid assigning Severity 1 solely to accelerate non-critical work.
- Maintain current authorized, technical and after-hours critical contacts as required by the subscribed support model.
- Provide timely information, evidence, access, approvals and testing reasonably required to investigate and resolve support conditions involving customer-managed dependencies.
- Protect customer-managed administrator identities and credentials and promptly notify PCL One of access changes that affect service operation or support.
- Maintain customer-managed systems and dependencies identified in the service design, including identity providers, networks, integration endpoints and required credentials.
- Participate in restoration, validation or recovery activities where customer action is reasonably required.

13. Assurance and evidence

PCL One maintains records supporting the operation of this policy. Detailed support 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.

- Support case records, severity classification and status history.
- Severity 1 acknowledgement and incident coordination records.
- Escalation records and relevant customer communications.
- Administrative-access and support-access records where applicable.
- Problem-management, root-cause and corrective-action records for material or recurring incidents.
- Support process metrics and service-management evidence where maintained for the subscribed service.

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.

14. Statement of changes

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