TRUST CENTRE

Security Incident & Breach Notification Policy

SECURITY INCIDENT RESPONSE AND CUSTOMER NOTIFICATION

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 approach to identifying, responding to and communicating security incidents that materially affect customer data or a contracted service. It is designed to support timely customer decision-making while allowing investigation, containment and recovery work to continue in parallel.

> **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 - managed cloud services and support operations where PCL One has responsibility for incident response involving customer data or service availability.

Covers customer-facing notification, response coordination, evidence preservation, recovery and post-incident follow-through.

Does not replace a customer's own statutory duties as controller, public body, regulated entity or employer.

Relationship to customer agreements

If this policy is incorporated by reference into a customer agreement or service schedule, it applies to the relevant service. Where the governing agreement, applicable law or regulator imposes a shorter or stricter notification obligation, that requirement prevails to the extent of conflict.

3. Definitions

Term	Meaning
Security Incident	An event that compromises, or is reasonably suspected to compromise, the confidentiality, integrity or availability of an in-scope PCL One service or customer data.
Confirmed Breach	A security incident confirmed to have resulted in unauthorized access to, acquisition of, use of or disclosure of customer data.
Material Incident	An incident confirmed to have a material impact on customer data or the contracted service, whether or not final breach classification is complete.
Customer Data	Data submitted to, stored in, or processed by the contracted PCL One service on the customer's behalf.

4. Incident response and notification

Notificationcommitments

Event	Baseline customer notification	Application
Confirmed breach affecting customer data	Within 12 hours of confirmation	A preliminary notice may be issued before the full forensic picture is known.

Event	Baseline customer notification	Application
Material customer-impacting incident	Without undue delay; target within 24 hours of confirmation of material customer impact	Used where material impact is confirmed while breach classification or full scope is still being established.
Personal-data breach subject to a shorter legal or contractual maximum	The shorter applicable timeline prevails	The governing agreement, applicable law or regulator requirement controls where stricter.

Initial notice content

Known nature of the incident and when it was detected or confirmed.

Affected service, environment and categories of customer data known at the time.

Known or reasonably suspected scope and customer impact.

Containment and recovery actions already taken or underway.

Any immediate action requested from the customer.

The next planned update point and the agreed customer contact channel.

Response lifecycle

Stage	Baseline control
Detect and triage	Validate the alert, classify severity, preserve relevant evidence and assign accountable incident ownership.
Contain	Limit further exposure or service impact using proportionate technical and access controls.
Investigate	Establish affected systems, data categories, timeline, root-cause indicators and reportability.
Notify	Contact designated customer contacts under the applicable notification baseline without waiting for perfect information.
Recover	Restore safe service, validate integrity and monitor for recurrence.
Close and improve	Provide post-incident findings when appropriate, track corrective actions and verify closure.

Customer coordination

Customer notifications are directed to the designated security, privacy and service contacts recorded for the engagement.

PCL One provides information reasonably available to support the customer's own regulator, data-subject, insurance or executive reporting obligations.

Where an underlying hosting or subprocessor incident is involved, PCL One coordinates the provider response and remains the customer-facing escalation point for the contracted service.

5. Customer responsibilities

Maintain current security, privacy and service contacts for incident communications.

Provide timely information and access reasonably required to investigate incidents involving customer-managed identities, networks, integrations or endpoints.

Determine and perform any notification obligations that apply directly to the customer as controller, public body, employer or regulated entity.

6. Exceptions and exclusions

Not every alert, vulnerability finding or service issue is a confirmed breach. Classification is based on available evidence and applicable definitions.

Incidents attributable to customer-managed systems or unrelated third parties are coordinated in good faith, but responsibility and service commitments remain subject to the governing agreement.

Law-enforcement, regulator or legal restrictions may limit the timing or content of specific disclosures where legally required.

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.

Incident timeline and case record.

Customer notification copies and status updates.

Relevant audit/access logs and evidence-preservation records.

Root-cause and corrective-action records for material incidents.

Incident-response exercise or test records where appropriate.

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.