TRUST CENTRE

Vulnerability Management & Disclosure Policy

VULNERABILITY IDENTIFICATION, PRIORITIZATION, REMEDIATION AND RESPONSIBLE REPORTING

Effective Date: 6 October 2025
Classification: Public
Document ID: PCL-TRUST-VULN-011

This document is intended for public distribution. Detailed vulnerability inventories, penetration-test findings, exploit evidence, internal scan results, remediation records, security architecture and other sensitive assurance material are restricted and may be provided separately to eligible customers, prospective customers, business partners, auditors or regulators subject to appropriate access and confidentiality restrictions.

Contents

This policy should be read together with the PCL One Information Security Practices, Secure Software Development Lifecycle Policy, Cloud Hosting & Delivery Policy, Security Incident & Breach Notification Policy and applicable customer agreement or Ordering Document.

1. Overview

This policy describes PCL One's baseline approach to identifying, assessing, prioritizing, remediating and tracking security vulnerabilities that may affect PCL One-managed cloud services, software, integrations and supporting technology. It also describes the public baseline for reporting suspected security vulnerabilities to PCL One.

Vulnerability management is risk-based. Technical severity is considered together with exploitability, exposure, affected data, service criticality, available mitigations and the operational risk of applying a change. The objective is to reduce security risk promptly while maintaining service stability and traceable change control.

Public baseline

PCL One does not publish a universal remediation-time commitment in this policy. Customer-specific remediation commitments, if any, are governed by the applicable agreement, Ordering Document, service schedule or expressly agreed security requirement.

2. Scope and applicability

This policy applies to PCL One-managed application code, configurations, infrastructure components, cloud services, APIs, integrations, deployment artifacts and material third-party dependencies where PCL One is responsible for vulnerability response or remediation.

Customer-controlled systems, customer-developed code, customer-managed integrations and third-party products outside PCL One control remain the responsibility of the applicable owner. PCL One may nevertheless coordinate triage, provider escalation or mitigation where an externally managed component affects a PCL One-managed service.

Related controls

- Secure design and development controls are defined in the Secure Software Development Lifecycle Policy.
- Production change, maintenance and emergency change controls are defined in the Cloud Hosting & Delivery Policy.
- Security incidents and confirmed breaches are handled under the Security Incident & Breach Notification Policy.
- Privileged access required for remediation is governed by the Privileged Support & Emergency Access Policy.

3. Vulnerability management principles

Principle	Baseline application
Risk based	Prioritize based on likely security impact rather than technical score alone.
Continuous inputs	Use multiple sources such as provider advisories, testing, scanning, monitoring, customer reports and research.
Defence in depth	Use permanent fixes or compensating controls to reduce exposure while remediation is planned or deployed.
Controlled change	Apply remediation through approved deployment, patching and emergency-change processes.
Traceability	Record material findings, decisions, exceptions, validation and closure evidence.
Need-to-know disclosure	Protect exploit details and sensitive findings while providing appropriate assurance to authorized recipients.

4. Sources of vulnerability information

PCL One may identify potential vulnerabilities through a combination of internal and external sources appropriate to the service and technology stack.

- Cloud, software, operating-system and technology-provider security advisories.
- Automated vulnerability, dependency, configuration or code scanning where implemented.
- Security testing performed during the software development lifecycle.
- Independent penetration testing, assurance reviews or audit activities where applicable.
- Operational monitoring, incident investigation and security-event analysis.
- Customer, partner or security-researcher reports.
- Defect reports, code review, threat analysis and engineering investigation.

- Industry alerts regarding actively exploited vulnerabilities or material supply-chain risk.

A reported issue is not treated as confirmed solely because a scanner, advisory or external report assigns a severity. PCL One validates applicability and affected scope before final prioritization where practical.

5. Assessment and prioritization

PCL One evaluates confirmed or credible vulnerabilities using available technical evidence and business context. CVSS or another recognized scoring method may be used as an input, but it does not replace contextual risk assessment.

Risk level	General characterization	Handling
Critical	Credible potential for severe compromise, broad unauthorized access, material data exposure, major service impact or active exploitation affecting a PCL One-managed service.	Expedited containment and remediation or mitigation.
High	Significant compromise potential or meaningful effect on confidentiality, integrity or availability with practical exploitation conditions.	Priority remediation with risk-reducing controls as needed.
Medium	Limited, constrained or lower-likelihood impact, or exploitation requiring material preconditions.	Planned remediation according to risk and release process.
Low	Minor weakness, defence-in-depth issue or limited practical security impact.	Address through normal maintenance, hardening or backlog management.

Contextual factors

- Known exploitation or credible public proof of concept.
- Internet exposure and accessibility of the affected component.
- Authentication, privilege, user interaction or network position required for exploitation.
- Sensitivity and volume of potentially affected customer or personal data.
- Service criticality and potential impact to confidentiality, integrity or availability.
- Availability and effectiveness of patches, mitigations, feature restrictions or compensating controls.
- Potential deployment, compatibility or operational risk created by remediation.

6. Remediation and mitigation

PCL One selects remediation actions that are proportionate to the vulnerability and the affected service. Permanent correction is preferred where practical, but temporary risk reduction may be used when a patch or permanent fix is not immediately available or would create unacceptable service risk.

Remediation method	Use
Software or dependency update	Apply a vendor or internally developed security fix.
Configuration hardening	Change service, identity, network or platform configuration to remove or reduce exposure.
Compensating control	Add monitoring, access restriction, filtering, isolation or other control that reduces exploitability or impact.
Feature restriction	Disable, limit or isolate affected functionality when necessary to protect customers or service integrity.
Provider escalation	Coordinate remediation with a cloud, software, platform or other service provider.
Service redesign	Modify architecture, data flow or implementation where a systemic weakness requires structural correction.

Urgent security remediation may use the emergency change path when delay could create greater customer or security risk than an expedited deployment. Emergency changes remain subject to authorization, recording, validation and retrospective review as applicable.

7. Patch and configuration management

Security patches, configuration changes and software updates are evaluated according to applicability, risk, service impact, vendor guidance and available mitigations. PCL One applies approved changes through controlled deployment or maintenance processes appropriate to the affected technology.

- Provider advisories are reviewed for applicability to PCL One-managed services where relevant.
- Security-sensitive changes are tested to the extent practical before production deployment.
- Where immediate patching is not practical, compensating controls may be used until a permanent fix is deployed.
- Planned customer-impacting maintenance is communicated under the Cloud Hosting & Delivery Policy and applicable customer terms.
- Emergency patching may proceed on an expedited basis when necessary to address material security risk.

8. Third-party components and provider vulnerabilities

PCL One services may depend on third-party software, cloud infrastructure, managed databases, libraries, packages, APIs or other providers. Vulnerabilities in those components are managed according to the responsibility PCL One holds for the affected layer.

PCL One may update a dependency, apply a configuration mitigation, restrict affected functionality, increase monitoring, isolate a component or escalate to the responsible provider. Where the provider controls the underlying remediation, PCL One tracks the issue and applies reasonable compensating controls available within PCL One control.

Provider responsibility

Use of a third-party provider does not remove PCL One responsibility for the controls and contractual obligations that PCL One has expressly accepted. The exact allocation of responsibility may depend on the service architecture and applicable customer terms.

9. Validation and closure

A vulnerability is closed when PCL One determines that the identified risk has been adequately remediated, mitigated, accepted or otherwise resolved according to the applicable risk decision. Closure evidence is proportionate to the finding and may include retesting, scan results, code review, configuration verification, deployment records or provider confirmation.

- Critical or material findings receive validation appropriate to the affected service and remediation method.
- Temporary mitigations are tracked for follow-up where a permanent fix remains outstanding.
- Reopened or recurring vulnerabilities are re-assessed using the current risk context.
- Lessons from material findings may be incorporated into development standards, hardening guidance, monitoring or architecture.

10. Coordinated vulnerability disclosure

PCL One welcomes good-faith reports of suspected security vulnerabilities affecting PCL One-managed services. Reports should be submitted through a designated PCL One security or customer-support channel published by PCL One or provided to the reporter through an existing customer relationship.

Information that helps investigation

- Affected service, URL, API, component or feature.
- A clear description of the suspected vulnerability and potential security impact.
- Reproduction steps, test conditions and relevant timestamps.
- Screenshots, request/response examples or other evidence that does not contain unnecessary personal or customer data.
- Reporter contact information for technical follow-up, where the reporter wishes to provide it.

Responsible testing expectations

- Do not intentionally access, alter, delete, exfiltrate or retain data belonging to another customer or individual.
- Do not perform denial-of-service, destructive testing, social engineering, credential attacks, spam, physical intrusion or testing that degrades production services.
- Use the minimum access and data necessary to demonstrate the issue and stop testing if sensitive or customer data is encountered.

- Do not publicly disclose exploit details before PCL One has had a reasonable opportunity to investigate and remediate or mitigate the issue.
- Do not represent that PCL One has authorized a bounty, payment, safe-harbor arrangement or other reward unless PCL One has expressly agreed to it in writing.

PCL One reviews reports for applicability and may request additional information. Public disclosure, if appropriate, is coordinated in light of remediation status, customer confidentiality, legal obligations and the risk of enabling exploitation.

11. Customer-reported security issues

Customers may report suspected vulnerabilities through their established support or security contact. A report that indicates active compromise, unauthorized access, material customer impact or suspected breach may be escalated into the Security Incident & Breach Notification process rather than handled solely as a vulnerability case.

PCL One may communicate relevant mitigation guidance, status or customer action through the applicable support or incident channel. Detailed exploit information, other-customer information and restricted security evidence are not disclosed except where PCL One determines that disclosure is appropriate and authorized.

12. Penetration testing and assurance

PCL One may use independent penetration testing, control testing, security assessment, code or dependency analysis and other assurance activities to evaluate the effectiveness of security controls. Scope, frequency and testing method may vary by service, architecture, risk profile and assurance program.

Detailed penetration-test reports and vulnerability findings are restricted because they can contain exploitable technical information. Eligible customers, prospective customers, auditors or regulators may receive an executive summary, attestation, remediation status or other appropriate evidence subject to confidentiality and access restrictions.

Customer testing

Customers must not conduct penetration testing, automated scanning or intrusive testing against PCL One-managed production services unless PCL One has expressly authorized the activity, scope, timing and conditions in writing.

13. Records, metrics and reporting

PCL One maintains records appropriate to material vulnerability-management activities. Depending on the issue and system, records may include the affected asset or component, source of the finding, assessment, severity, assigned owner, remediation or mitigation action, exception decision, validation and closure evidence.

- Metrics may be used to monitor open risk, aging, recurrence, control effectiveness and remediation trends.
- Detailed vulnerability inventories and finding-level reports are restricted assurance material.
- Material trends may be reviewed by security, engineering, operations or governance functions and used to improve controls.
- Records are retained according to applicable operational, security, legal and assurance requirements.

14. Exceptions and risk acceptance

A vulnerability may remain open when immediate remediation is not technically available, would create disproportionate service risk, depends on a third-party provider or is otherwise subject to a documented exception. Material exceptions require risk assessment, an accountable owner, documented rationale and compensating controls where appropriate.

Risk acceptance does not eliminate the underlying vulnerability. Accepted risk should be reviewed when material circumstances change, such as new exploitation evidence, increased exposure, new customer impact, a vendor fix becoming available or expiration of the approved exception period.

15. Statement of changes and related documents

Statement of changes

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

Related documents

Document	Relationship
PCL One Information Security Practices	Enterprise security governance and vulnerability-management baseline.
PCL One Secure Software Development Lifecycle Policy	Secure design, testing, dependency and release controls.
PCL One Cloud Hosting & Delivery Policy	Operational maintenance, change and emergency-change controls.
PCL One Security Incident & Breach Notification Policy	Escalation and notification when a vulnerability is associated with a security incident or breach.
PCL One Privileged Support & Emergency Access Policy	Controls for privileged access used during investigation or remediation.
PCL One Subprocessor & Third-Party Services Policy	Governance of third-party services and providers.