TRUST CENTRE

Secure Software Development Lifecycle Policy

SECURE DESIGN, DEVELOPMENT, TESTING, RELEASE AND MAINTENANCE

Effective Date: 6 October 2025
Classification: Public
Document ID: PCL-TRUST-SDLC-012

This document is intended for public distribution. Detailed source code, security test results, vulnerability records, deployment configurations, architecture details and other sensitive assurance material may be provided separately to eligible customers, prospective customers, business partners or regulators subject to appropriate access and confidentiality restrictions.

Contents

This policy should be read together with the PCL One Information Security Practices, Cloud Hosting & Delivery Policy, Security Incident & Breach Notification Policy, Privileged Support & Emergency Access Policy, Data Processing Addendum and applicable customer agreement or Ordering Document.

1. Overview

This policy describes PCL One's baseline secure software development lifecycle (SDLC) practices for software, services, integrations and material changes that PCL One designs, develops, configures or maintains for PCL One-managed cloud services. The objective is to reduce security and privacy risk throughout the lifecycle, from requirements and design through release, operation and retirement.

Security is treated as a lifecycle responsibility rather than a single pre-release activity. The depth of controls and testing is proportionate to the nature of the change, service exposure, data sensitivity, customer impact and identified threat or vulnerability risk.

Public baseline
This policy describes PCL One's standard approach. A customer agreement, Ordering Document, service schedule, security requirement or applicable law may establish additional or stricter controls for a specific service or customer deployment.

2. Scope and applicability

This policy applies to PCL One-managed application code, configuration, APIs, integrations, automation, infrastructure-as-code and deployment activities where PCL One controls the development or release process. It also applies, as relevant, to material changes to production services and supporting non-production environments.

Customer-developed code, customer-managed integrations, third-party products and infrastructure outside PCL One's control are governed by the responsible party. PCL One may nevertheless apply integration, security review or change controls where those components connect to a PCL One-managed service.

Related controls

- Information security governance, identity, access control, encryption and monitoring are governed by the PCL One Information Security Practices.
- Production change, maintenance and service delivery controls are also governed by the Cloud Hosting & Delivery Policy.
- Security incidents and confirmed breaches are handled under the Security Incident & Breach Notification Policy.
- Privileged or emergency production access is governed by the Privileged Support & Emergency Access Policy.

3. Secure development principles

PCL One applies the following principles to software and service development activities:

Principle	Baseline application
Security by design	Security, privacy, availability and supportability considerations are addressed during requirements and design rather than deferred until release.
Least privilege	Users, service identities, repositories, build systems and deployment mechanisms are granted only the access needed for their function.
Separation of environments	Development, testing and production environments are separated, and promotion into production follows controlled release processes.
Defence in depth	Application, identity, network, data and monitoring controls are layered so that the failure of one control does not become the sole barrier to compromise.
Traceability	Material changes, approvals, test results and deployments are recorded at a level appropriate to the service and change risk.
Risk-based remediation	Security defects and vulnerabilities are prioritized based on severity, exploitability, exposure, affected data and customer impact.

4. Roles and separation of duties

Development and release responsibilities are assigned so that no individual requires unrestricted access across all lifecycle stages. PCL One uses role-based access and review or approval controls appropriate to the service and change risk.

Role	Responsibility
Product / business owner	Defines business requirements, service impact and acceptance criteria.
Engineering / configuration team	Implements approved changes and maintains technical documentation and evidence appropriate to the change.
Reviewer / approver	Performs technical, functional or security review as required by the change class.
Operations / release function	Controls or oversees production deployment, monitoring and rollback activities where applicable.
Security / risk function	Provides security requirements, risk review, vulnerability oversight and exception governance where required.

Where team size or service design makes strict personnel separation impractical, compensating controls may include documented peer review, change approval, deployment logging, time-limited privileged access and retrospective review.

5. Security requirements and design

Security requirements are identified from service architecture, customer and regulatory obligations, data classification, integration patterns and reasonably foreseeable misuse or threat scenarios. Design review is proportionate to the risk and may include application, API, identity, network, data and operational considerations.

Common design considerations

- Authentication, authorization, role-based access and segregation of duties.
- Input validation, output handling and protection against common injection and browser-based attack patterns.
- API authentication, authorization, rate or abuse controls and secure integration patterns.
- Encryption in transit and at rest, key or secret handling, and sensitive-data minimization.
- Tenant or customer data separation, audit logging and traceability.
- Availability, failure handling, recovery, backup dependencies and operational monitoring.
- Privacy requirements, retention, deletion and restrictions on the use of production data.
- Third-party libraries, services and dependencies that could affect security or service continuity.

PCL One considers recognized application-security risk categories, including the OWASP Top 10 and equivalent industry guidance, as inputs to design, review and testing. Reference to such guidance does not represent a certification unless expressly stated in an applicable assurance report or customer agreement.

6. Source code and repository controls

PCL One-managed source code and configuration are maintained in controlled repositories or equivalent managed systems. Access is restricted to authorized personnel and is reviewed or removed when no longer required.

- Changes are associated with a work item, issue, release record or equivalent traceable business or technical purpose where appropriate.
- Review and approval controls are applied in proportion to the risk of the change before production release.
- Production credentials, private keys and other long-lived secrets are not intended to be stored in source code. Secrets are managed through approved secure mechanisms appropriate to the service.
- Repository and deployment permissions are limited according to role and operational need.
- Material security-relevant changes are retained in change history or equivalent records to support investigation and assurance.

7. Third-party components and dependencies

Third-party software, open-source components, libraries, packages, services and build dependencies can introduce security and supply-chain risk. PCL One manages such risk according to the component's function, service exposure and availability of vendor or community security information.

- Components are obtained from approved or reputable sources appropriate to the technology stack.
- Versions and material dependencies are tracked at a level sufficient to support maintenance, security review and incident response.
- Security advisories and known vulnerabilities are evaluated through vulnerability-management processes, automated tooling, vendor notification, manual review or equivalent controls as appropriate.

- Unsupported or end-of-life components are replaced, upgraded, isolated or otherwise risk-managed according to service impact and available alternatives.
- Subprocessors or external hosted services that process customer data remain subject to PCL One's third-party and data-protection governance.

8. Security testing and verification

Changes are tested before production release at a level proportionate to their scope and risk. Testing may combine automated and manual methods and is intended to identify functional defects, security weaknesses, regression risk and release issues before customer impact occurs.

Control	Purpose
Functional and regression testing	Validates expected behavior and checks that existing functionality is not materially impaired by the change.
Code or configuration review	Examines material changes for correctness, security impact, maintainability and compliance with approved patterns where applicable.
Application security testing	May include static analysis, dynamic testing, dependency or composition analysis, API testing, configuration scanning or equivalent techniques based on the service and change risk.
Vulnerability assessment	Evaluates identified vulnerabilities, affected assets, exploitability and required remediation or compensating controls.
Penetration or independent testing	Performed according to the assurance program, service risk, customer commitments or regulatory requirements; detailed results are restricted information.
Release validation	Confirms deployment readiness, rollback considerations, monitoring and operational support requirements before or immediately after release.

Testing scope

Not every test method is applicable to every change or service. PCL One selects testing techniques based on technology, exposure, data sensitivity, service criticality and the type of change being released.

9. Environment separation and data handling

Development, test and production environments are logically separated according to the architecture of the service. Access to production is more restricted than routine development access and is governed through operational and privileged-access controls.

- Changes are validated in non-production environments before production promotion where the nature of the service permits.
- Production customer data is not used in development or test environments unless there is an approved business need and appropriate protection, authorization and data-handling controls are applied.
- Where production-like data is required for testing, minimization, masking, synthetic data, controlled extracts or equivalent safeguards are used where practical and appropriate.
- Non-production environments that contain customer data remain subject to applicable access, security, retention and incident-management controls.

10. Build, release and deployment controls

Production releases are performed through controlled deployment processes. The exact workflow varies by service architecture, but PCL One maintains change traceability and operational controls designed to reduce unauthorized or untested production change.

Release stage	Baseline control
Change identification	Record the business or technical purpose, scope and affected service or component.
Risk and impact review	Assess customer impact, security implications, dependencies, maintenance needs and rollback considerations.

Release stage	Baseline control
Testing	Complete applicable functional, regression, integration and security validation.
Approval	Obtain required technical, business, security or operational approval based on change class.
Deployment	Use authorized deployment mechanisms and restricted production access.
Validation and monitoring	Confirm service health, review alerts or errors and activate rollback or incident procedures when required.

Release communications, planned maintenance and customer notifications are governed by the Cloud Hosting & Delivery Policy and applicable customer terms.

11. Vulnerability and defect management

Security vulnerabilities and defects identified through testing, monitoring, vendor advisories, customer reports, security research or incident response are recorded and evaluated according to risk. PCL One does not publish a universal remediation-time commitment in this policy unless a customer agreement or service schedule establishes one.

Risk evaluation factors

- Technical severity and credible exploitability.
- Internet exposure, affected interfaces and required attacker access.
- Whether exploitation is known or actively occurring.
- Customer-data sensitivity, privilege level and potential confidentiality, integrity or availability impact.
- Availability of vendor fixes, mitigations, configuration controls or compensating safeguards.
- Service criticality, deployment risk and the potential effect of remediation itself.

Critical or otherwise urgent vulnerabilities are prioritized for expedited action. Remediation may include patching, configuration change, feature restriction, compensating control, isolation, vendor escalation or other risk-reduction measures until permanent correction is available.

12. Change and emergency change management

Routine changes follow the standard review, testing, approval and deployment process. Emergency changes may use an expedited path when required to restore service, contain an incident, remediate an urgent vulnerability or prevent material customer impact.

Emergency changes remain subject to authorization, change recording and validation to the extent feasible during the event. A retrospective review is performed where appropriate to confirm the result, identify follow-up work and ensure that temporary controls or elevated access are removed when no longer required.

13. Logging, monitoring and post-release response

PCL One uses service and security monitoring to identify deployment failures, anomalous behavior, service degradation and security events after release. Relevant logs and deployment records are retained according to applicable operational, security and data-retention requirements.

- Post-release issues are triaged through support, operations, engineering or incident-management processes according to impact.
- Security events are escalated to the Security Incident & Breach Notification process where the applicable incident criteria are met.
- Lessons from incidents, material defects, failed changes or assurance findings may be incorporated into development standards, testing practices or release controls.
- Where rollback is appropriate and technically feasible, PCL One may restore a prior version, disable affected functionality or use another controlled recovery method.

14. Assurance evidence and customer requests

PCL One may provide appropriate evidence of secure development practices to customers, prospective customers, auditors or regulators where reasonably required and subject to confidentiality, security and access restrictions. Evidence may include policy excerpts, development-control descriptions, change-management evidence, testing summaries, independent assurance reports or selected remediation evidence.

Source code, detailed penetration-test findings, vulnerability inventories, credentials, internal architecture details and security configurations are not public documents and are disclosed only where PCL One determines that the recipient has a legitimate need and appropriate protections are in place.

Customer responsibilities

- Customers are responsible for securely developing and maintaining customer-controlled code, scripts, configurations and integrations unless PCL One has expressly accepted that responsibility.
- Customers must protect credentials, API keys and integration secrets under their control and promptly report suspected compromise.
- Customers should test customer-managed integrations and configuration changes before production use and follow applicable change-management requirements.

15. Exceptions and statement of changes

Exceptions

Exceptions to this policy require documented business or technical justification, assessment of security risk, approval by an authorized owner and compensating controls where appropriate. Exceptions should be time-limited or reviewed periodically when the underlying condition persists.

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 baseline controls.
PCL One Cloud Hosting & Delivery Policy	Hosting, operations, change management and service delivery controls.
PCL One Security Incident & Breach Notification Policy	Security incident classification, escalation and customer notification.
PCL One Privileged Support & Emergency Access Policy	Privileged and break-glass access controls.
PCL One Data Processing Addendum	Processing, security and data-protection obligations.
PCL One Subprocessor & Third-Party Services Policy	Third-party service and subprocessor governance.