

TRUST CENTRE

Release, Change & Maintenance Policy

SERVICE RELEASES, PRODUCTION CHANGES, MAINTENANCE, DEPRECATION AND CUSTOMER COMMUNICATION

Effective Date: 6 October 2025

Classification: Public

Document ID: PCL-TRUST-CHG-007

This document is intended for public distribution. Detailed production runbooks, deployment pipelines, internal approval records, rollback procedures, monitoring thresholds, infrastructure diagrams and security-sensitive change evidence are restricted and may be provided separately to eligible customers, auditors or regulators subject to appropriate access and confidentiality restrictions.

Contents

This policy should be read together with the PCL One Cloud Hosting & Delivery Policy, Secure Software Development Lifecycle Policy, Vulnerability Management & Disclosure Policy, Cloud Service Availability SLA, Cloud Support Policy, Service Resilience & Recovery Policy, applicable Service Description and the customer Ordering Document or Service Schedule.

01	Overview
02	Scope and applicability
03	Change management principles
04	Change categories and risk
05	Release lifecycle
06	Testing, approval and production promotion
07	Planned maintenance
08	Emergency and security changes
09	Customer communications
10	Compatibility, integrations and customer action
11	Deprecation and end of service features
12	Business-critical periods and change freezes
13	Third-party and infrastructure changes
14	Availability, support and incident coordination
15	Customer responsibilities
16	Assurance, exceptions and related documents
17	Statement of changes

1. Overview

PCL One manages service releases, production changes and maintenance through controlled processes intended to protect service availability, security, data integrity and customer operations. The level of review, testing, approval and customer communication is proportionate to the risk and expected impact of the change.

Public baseline

Planned customer-impacting maintenance is communicated in advance where practicable. Specific maintenance windows, notice periods, blackout periods or release commitments are governed by the applicable Order, Service Schedule or Service Availability SLA. Emergency and security changes may require shorter notice or immediate action.

2. Scope and applicability

This policy applies to PCL One-controlled changes affecting production cloud services, including application releases, configuration changes, infrastructure maintenance, security remediation, database and platform changes, integrations managed by PCL One and material changes to service dependencies.

- Customer-controlled configuration, customer endpoints and customer-managed integrations remain the Customer's responsibility unless PCL One is expressly engaged to manage them.
- Service-specific release schedules and maintenance requirements may differ by product, hosting model, provider or customer agreement.
- Where an Order, Service Schedule, SLA or approved project plan contains a more specific change or maintenance commitment, that document controls for the applicable service.

3. Change management principles

- Changes are authorized, traceable and associated with an identified business, security, reliability or compliance purpose.
- The potential impact on availability, security, privacy, data integrity, integrations and customer operations is considered before production deployment.
- Development, testing and production activities are separated through appropriate access and environment controls.
- Testing and deployment evidence is retained to a level appropriate to the change risk and applicable assurance requirements.
- Changes are monitored after deployment so unexpected behavior can be detected and addressed promptly.
- Rollback, remediation or forward-fix options are considered for material changes where technically feasible.

4. Change categories and risk

Change category	Typical treatment
Standard / routine	Repeatable, lower-risk activity performed under an approved procedure. May use pre-authorized implementation steps and routine validation.
Normal / planned	Assessed before implementation for impact, dependencies, testing, approval, timing and communication requirements.
Major / high-impact	Receives enhanced impact assessment, testing, approval, deployment planning and customer coordination where the change could materially affect service behavior or availability.
Emergency / security	Expedited change used to address an active incident, critical vulnerability, provider emergency or material service risk. Review and documentation may be completed or supplemented after immediate stabilization where necessary.

Change classification is based on risk and impact, not solely on the size of the code or configuration change.

5. Release lifecycle

PCL One applies a controlled lifecycle to material service releases. The exact workflow may vary by product and delivery model, but generally includes the following activities:

- Define the purpose, scope, affected service components and dependencies.
- Assess security, privacy, availability, data, integration and operational impact.

- Develop or configure the change under controlled source, configuration and access-management practices.
- Test in an appropriate non-production environment and resolve material defects before production promotion.
- Obtain required technical or operational approval before deployment.
- Deploy using controlled procedures, monitor service behavior and close the change after validation.
- Capture release information or customer-facing notes when the change materially affects customer use, administration or integration.

6. Testing, approval and production promotion

Production promotion is performed by authorized personnel or approved automated processes. Testing depth is proportionate to the change and may include functional, regression, integration, security, performance, migration or recovery validation as applicable.

- Material application changes follow the PCL One Secure Software Development Lifecycle Policy.
- Security findings are prioritized and remediated under the Vulnerability Management & Disclosure Policy.
- Production credentials, secrets and privileged permissions are controlled separately from routine development access.
- Where a change modifies data structures, interfaces or migration behavior, validation includes data integrity and recoverability considerations appropriate to the service.

7. Planned maintenance

Planned maintenance may be required for application releases, infrastructure work, database operations, platform upgrades, security hardening or provider maintenance. PCL One seeks to schedule customer-impacting maintenance to reduce operational disruption while preserving security and service reliability.

- Maintenance that is expected to materially affect service availability is communicated through the designated customer communication channel in advance where practicable.
- The notice period and maintenance window, where contractually committed, are identified in the applicable Order, Service Schedule or SLA rather than established as a universal public timer.
- Some maintenance can be completed without customer-visible interruption and may not require a customer notice.
- Scheduled downtime is treated for availability measurement according to the applicable Service Availability SLA.

8. Emergency and security changes

PCL One may implement emergency maintenance or security changes when delay would create unacceptable risk to confidentiality, integrity, availability, legal compliance or service continuity. Examples include active exploitation, critical vulnerabilities, severe service degradation, provider emergencies or urgent infrastructure protection.

Emergency notice

Emergency changes may be implemented with shortened notice or without advance notice when immediate action is reasonably necessary. PCL One communicates material customer impact as soon as practicable through the applicable incident, support or service-notification process.

9. Customer communications

Customer communication is proportionate to the expected impact of the change. Depending on the service and change type, communication may include maintenance notices, release notes, support notifications, status communications, account-team notices or service-specific documentation.

Communication circumstance	Typical information
Planned customer-impacting maintenance	Expected timing, affected service or function, anticipated impact and any customer action known at the time.
Material feature or behavior change	Summary of the change, intended customer benefit or impact, relevant documentation and any required preparation.
Emergency change	Known impact, mitigation status and follow-up information when advance notice is not practicable.
Customer action required	Required action, applicable deadline or dependency, compatibility information and support path where available.

10. Compatibility, integrations and customer action

PCL One considers compatibility with supported interfaces, integrations and service behavior when planning material changes. Because cloud services and third-party dependencies evolve, perpetual compatibility with every historical implementation or external component is not guaranteed unless expressly committed in the applicable service documentation.

- Where a material change requires customer action, PCL One seeks to identify the action and timing through appropriate service communications.
- Customers are responsible for maintaining supported browsers, endpoints, credentials, network access and customer-controlled integration components.
- Customer-developed integrations should use documented interfaces and supported authentication methods to reduce upgrade risk.

11. Deprecation and end of service features

PCL One may retire, replace or materially redesign features as services evolve. For material customer-facing deprecations, PCL One seeks to provide reasonable advance communication appropriate to the service, the nature of the change, contractual requirements and security considerations.

- A specific notice period applies only where stated in the applicable Order, Service Schedule, service description or other governing commitment.
- Security, legal or provider-driven circumstances may require accelerated retirement or restriction of unsafe or unsupported functionality.
- Where practicable, communications identify replacement functionality, migration considerations or customer actions relevant to continued use.

12. Business-critical periods and change freezes

Some customers operate business-critical periods such as payroll processing, taxation, billing, fiscal year-end or statutory filing windows. Where such periods are documented in the applicable project plan, Order or Service Schedule, PCL One considers them when scheduling discretionary customer-impacting changes.

- Change freezes or blackout periods are customer-specific and are not implied unless documented and agreed.
- Emergency security, incident-response or provider-required changes may still be necessary during a blackout period when postponement would create greater risk.

13. Third-party and infrastructure changes

PCL One services may depend on approved cloud infrastructure, database, identity, communications, AI or other service providers. Provider changes may influence maintenance timing, supported capabilities or underlying infrastructure behavior.

- PCL One assesses material provider changes for security, privacy, availability, residency and service impact as applicable.
- Subprocessor or location changes are governed by the PCL One Subprocessor & Third-Party Services Policy, Data Processing Addendum and any customer-specific notice or objection rights.
- Provider emergency maintenance may require PCL One to coordinate or implement related service changes on an expedited basis.

14. Availability, support and incident coordination

Change management is coordinated with service availability, support and incident processes. A failed or degraded change may be treated as an operational incident and escalated according to the Cloud Support Policy and Security Incident & Breach Notification Policy where applicable.

- Availability calculations and planned-maintenance exclusions are governed by the Cloud Service Availability SLA.
- Severity classifications and support response commitments are governed by the Cloud Support Policy and applicable customer support schedule.
- Recovery objectives are governed by the Service Resilience & Recovery Policy and applicable Service Schedule; they are not promises that every failed change will be reversed within the RTO or RPO.

15. Customer responsibilities

- Maintain current administrative and technical contacts for maintenance and release communications.

- Review release or maintenance notices that identify required customer action and complete such action within the stated timeframe.
- Identify material blackout periods, regulatory constraints or integration dependencies during contracting or implementation so they can be documented where required.
- Test customer-managed integrations and local processes when a communicated change could affect them.
- Maintain supported customer-controlled software, network paths, browsers, endpoints and identity configurations.
- Raise suspected change-related service issues through the designated support channel with relevant timestamps and impact information.

16. Assurance, exceptions and related documents

PCL One maintains records appropriate to the risk of material production changes, which may include approvals, test evidence, deployment information, monitoring results and post-change review. Detailed change tickets, internal logs, source repositories, pipeline configurations and infrastructure runbooks are restricted because they may contain sensitive operational or security information.

Document	Relationship
PCL One Cloud Hosting & Delivery Policy	Hosting operations, maintenance, service delivery and change-management framework.
PCL One Secure Software Development Lifecycle Policy	Secure design, development, testing and controlled production promotion.
PCL One Vulnerability Management & Disclosure Policy	Security findings, remediation, patching and risk-based treatment.
PCL One Cloud Service Availability SLA	Availability measurement, scheduled downtime and service-level treatment.
PCL One Cloud Support Policy	Support channels, severity handling and escalation for change-related service issues.
PCL One Service Resilience & Recovery Policy	Recovery objectives and continuity controls for declared recovery events.

Exceptions

Any exception to required change controls, customer-specific notice periods or approved blackout commitments must be authorized through the applicable governance and contractual process. Operational convenience alone does not override a documented customer commitment.

17. Statement of changes

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

This public policy describes PCL One's baseline approach. The applicable Cloud Services Agreement, Ordering Document, Service Schedule, Service Availability SLA and customer-specific project or support documentation govern where they contain more specific commitments.