TRUST CENTRE

Encryption & Key Management Policy

ENCRYPTION, CRYPTOGRAPHIC KEY LIFECYCLE, SECRET PROTECTION AND ACCESS CONTROL

Effective Date: 6 October 2025
Classification: Public
Document ID: PCL-TRUST-ENC-009

This document is intended for public distribution. Detailed key inventories, key identifiers, secret locations, cryptographic configuration, access logs, recovery material and other sensitive technical 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 Information Security Practices, Cloud Hosting & Delivery Policy, Secure Software Development Lifecycle Policy, Data Retention, Backup & Secure Disposal Policy, Privileged Support & Emergency Access Policy and applicable customer agreement or Ordering Document.

01 Overview
02 Scope and applicability
03 Encryption and cryptographic principles
04 Encryption in transit
05 Encryption at rest
06 Cryptographic algorithms and protocols
07 Key lifecycle management
08 Secrets and credentials
09 Backups, exports and removable copies
10 Tokenization and masking
11 Third-party and cloud-provider key services
12 Access to keys and cryptographic material
13 Rotation, revocation and recovery
14 Logging and monitoring
15 Customer-managed encryption options
16 Suspected key compromise
17 Assurance, exceptions and related documents

1. Overview

PCL One uses encryption and related cryptographic controls to protect the confidentiality and integrity of customer information while it is transmitted, stored, backed up and processed within PCL One-managed services. Cryptographic controls are selected and operated according to the sensitivity of the information, the service architecture, applicable contractual commitments and the capabilities of the underlying technology provider.

Public baseline

PCL One customer data is protected in transit using TLS 1.2 or higher where PCL One controls the connection and is encrypted at rest using AES-256 or equivalent platform-provided encryption controls for applicable production storage. More specific service commitments, if any, are stated in the applicable Order or Service Description.

2. Scope and applicability

This policy applies to PCL One-managed production services, supporting infrastructure, backups, administrative tooling and development or operational processes where PCL One is responsible for selecting, configuring or governing encryption and cryptographic key controls.

- Customer-managed systems, endpoints and networks remain subject to customer security responsibilities unless expressly included in the applicable service scope.
- Where a cloud or third-party provider performs underlying encryption or key-management functions, PCL One governs the configuration and access within PCL One responsibility.
- Service-specific or customer-specific encryption requirements in an applicable agreement, Order, Service Description, DPA or approved technical design take precedence over this public baseline where they are more specific.

3. Encryption and cryptographic principles

- Use cryptography to reduce the risk of unauthorized disclosure or alteration of sensitive information.
- Use current, industry-recognized algorithms, protocol versions and platform security capabilities appropriate to the service.
- Separate access to cryptographic material from ordinary application and user access where the architecture supports that separation.
- Restrict key, secret and credential access according to least privilege, need to know and role-based authorization.
- Do not embed production secrets, private keys or credentials in source code, public repositories, documentation or client-side application content.
- Rotate, revoke or replace cryptographic material when required by security events, lifecycle controls, provider guidance or approved operating procedures.
- Keep detailed key-management implementation information restricted because disclosure can increase security risk.

4. Encryption in transit

PCL One protects network communications containing customer information through encrypted transport when PCL One controls the applicable endpoint or connection. TLS is the standard protection for browser, API and service-to-service connections exposed through PCL One-managed interfaces.

Control area	Public baseline
External web and API traffic	TLS 1.2 or higher for PCL One-managed customer-facing connections.
Administrative access	Encrypted remote-access protocols and authenticated administrative channels appropriate to the managed platform.
Service-to-service traffic	Encrypted transport is used where supported and appropriate to the sensitivity, trust boundary and platform architecture.
Legacy or third-party endpoints	Connections that cannot meet the normal baseline require documented assessment, approved exception or compensating control before production use.

PCL One may disable or restrict deprecated protocol versions, weak cipher suites or insecure connection methods when necessary to maintain the security of the service.

5. Encryption at rest

Applicable production customer data is encrypted at rest using AES-256 or equivalent encryption provided by the approved storage or cloud platform. The exact mechanism may vary by database, object storage, managed service, backup system or other component.

- Production databases and persistent storage containing customer data use platform or service encryption appropriate to the component.
- Backups and recovery copies containing customer data are protected using encryption and access controls consistent with the approved backup architecture.
- Temporary files, caches and derived data are minimized and protected according to their sensitivity and technical role.
- Non-production environments may use representative, masked, synthetic or appropriately protected data according to development and testing needs and applicable restrictions.

6. Cryptographic algorithms and protocols

PCL One favors cryptographic algorithms and protocol versions that are broadly recognized as suitable for modern commercial cloud services. Algorithm selection may be implemented through managed cloud services, application frameworks, operating systems, databases or approved cryptographic libraries.

PCL One reviews material changes in platform guidance, security standards, vendor support and known cryptographic weaknesses. Deprecated or materially weakened algorithms and protocols are removed, disabled or mitigated according to risk and technical feasibility.

Implementation detail

This public policy states security outcomes rather than a complete cipher or algorithm inventory. Detailed cryptographic configuration is restricted security information and may change as platforms and standards evolve.

7. Key lifecycle management

Cryptographic keys used within PCL One-managed services are governed across their lifecycle according to the function of the key, sensitivity of the protected information, provider capabilities and service architecture.

Lifecycle stage	Control objective
Generation	Keys are generated using approved platform or cryptographic services designed for the intended security purpose.
Storage	Keys and key material are stored separately from ordinary application data where supported and protected against unauthorized access or disclosure.
Use	Key use is limited to authorized services, identities and approved operational purposes.
Rotation	Keys are rotated according to platform capabilities, security requirements, operational risk and event-driven needs.
Revocation	Keys are disabled, revoked or replaced when they should no longer be trusted or used.
Retirement	Retired key material is retained only as needed for legitimate recovery, decryption, legal or operational requirements and is otherwise securely disposed of in accordance with approved procedures.

8. Secrets and credentials

Passwords, API keys, access tokens, certificates, private keys and other secrets are treated as sensitive authentication or cryptographic material. Production secrets must not be intentionally committed to public source repositories or embedded in documentation intended for broad distribution.

- Access is limited to authorized personnel, services or workloads with a legitimate operational need.
- Secrets should be held in approved platform secret-management, credential-management or protected configuration mechanisms where technically available.
- Administrative credentials are subject to the Privileged Support & Emergency Access Policy and related access-control requirements.
- A suspected exposed or compromised secret is replaced or revoked promptly according to the risk and service impact.

- Shared or long-lived credentials are avoided where practical in favor of named identities, scoped credentials and managed service identities.

9. Backups, exports and removable copies

Customer data may exist in backups, exports, reports, diagnostic material or other controlled copies. PCL One applies encryption and access controls appropriate to the copy, its sensitivity and its intended use.

- Backup encryption is part of the approved backup and recovery design for customer data.
- Customer-requested exports are delivered through approved channels and remain subject to the applicable agreement, retention requirements and customer responsibilities after delivery.
- Restricted diagnostic or support copies are minimized, access-controlled and removed when no longer required.
- Use of removable media for customer data is restricted and subject to approved security and disposal procedures.

10. Tokenization and masking

PCL One may use tokenization, masking, redaction, field-level protection or similar techniques to reduce exposure of sensitive values in selected workflows. These controls supplement, rather than replace, encryption where encryption is otherwise required.

For services handling highly sensitive identifiers, selected fields such as bank information, tax identifiers or other personal data may be masked or tokenized according to the application design. The exact fields and method depend on the product, feature and service configuration.

11. Third-party and cloud-provider key services

PCL One may rely on approved cloud infrastructure, managed databases, storage services, certificate authorities or other providers to perform underlying encryption, key storage or cryptographic operations. Such providers remain subject to PCL One third-party governance within the scope of PCL One responsibility.

The use of a managed provider does not remove PCL One responsibility for configuration, access control and contractual commitments that PCL One has expressly accepted. Provider-specific key architecture, service locations and responsibilities may be described in the applicable Service Description, Subprocessor Register or customer documentation.

12. Access to keys and cryptographic material

Access to cryptographic keys, private key material, protected secrets and related administration functions is restricted to authorized identities with a legitimate operational need. Access is governed using least privilege, role-based authorization and privileged-access controls appropriate to the platform.

- Administrative access uses named identities and multi-factor authentication where supported and required by the platform.
- Routine support personnel do not receive broad standing access to cryptographic material solely because they provide customer support.
- Privileged or emergency access is time-bounded or otherwise controlled where the platform supports elevation workflows.
- Key-management and secret-management actions are logged or auditable where supported by the underlying platform.

13. Rotation, revocation and recovery

Key rotation and replacement may be scheduled, provider-managed or event-driven. PCL One may rotate, revoke or replace cryptographic material following personnel changes, suspected compromise, security incidents, certificate expiry, provider recommendations, architecture changes or other material risk events.

Where recovery of encrypted information depends on key availability, PCL One uses platform and operational controls designed to preserve legitimate recovery capability without creating uncontrolled copies of key material. Detailed recovery mechanisms are restricted security information.

14. Logging and monitoring

PCL One monitors security-relevant administrative activity and platform events according to the capabilities of the service. Logging may include access to secret-management or key-management functions, authentication events, configuration changes, certificate lifecycle events and other security-relevant actions.

Logs and alerting support investigation, access review, anomaly detection and incident response. Detailed key-access logs and cryptographic event records are restricted assurance material and are not published as part of this policy.

15. Customer-managed encryption options

Customer-managed keys, bring-your-own-key arrangements, dedicated key scopes or other advanced encryption configurations are not represented by this policy as universally available features. Where such an option is offered for a particular service, its architecture, responsibilities, limitations, support model and recovery implications are documented in the applicable Order, Service Description or technical design.

Customer responsibility

Where a customer controls or supplies encryption keys, the customer may be responsible for key availability, rotation, authorization and recovery actions. Loss, revocation or misconfiguration of a customer-controlled key may make protected data or services unavailable.

16. Suspected key compromise

A suspected compromise of encryption keys, private keys, certificates, credentials or other critical cryptographic material is treated as a security event and assessed according to the Security Incident & Breach Notification Policy. Response actions may include revocation, rotation, certificate replacement, credential reset, access restriction, enhanced monitoring and investigation of affected systems or data.

Customer notification is governed by the applicable incident policy, law and contract. The existence of a key or secret exposure does not by itself determine whether customer data was accessed; PCL One evaluates the circumstances and available evidence.

17. Assurance, exceptions and related documents

Assurance and evidence

Evidence supporting encryption and key-management controls may include configuration records, provider security documentation, access logs, control-test evidence, architecture material and independent assurance reports. Detailed evidence is restricted and may be made available to eligible customers, auditors or regulators under appropriate confidentiality and access controls.

Exceptions

Exceptions to the normal encryption or key-management baseline require documented assessment and approval appropriate to the risk. Exceptions should identify the affected service or data, rationale, compensating controls, accountable owner and review or expiry condition. More specific contractual or legal obligations remain controlling.

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, access control and data-protection baseline.
PCL One Cloud Hosting & Delivery Policy	Hosting, platform security, operational controls and service delivery.
PCL One Secure Software Development Lifecycle Policy	Secure development, secret handling and release controls.
PCL One Privileged Support & Emergency Access Policy	Privileged administrative and emergency access controls.
PCL One Data Retention, Backup & Secure Disposal Policy	Backup protection, retention and secure disposal requirements.
PCL One Security Incident & Breach Notification Policy	Response and notification for suspected compromise or unauthorized access.