TRUST CENTRE

Information Security Practices

SECURITY GOVERNANCE, ACCESS CONTROL, DATA PROTECTION AND ASSURANCE

Effective Date: 6 October 2025

Classification: Public

Document ID: PCL-TRUST-SEC-010

This document is intended for public distribution. Detailed security architecture, testing evidence, account identifiers, configuration records 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 applicable Cloud Services Agreement, Ordering Document, Cloud Service Description, Cloud Hosting & Delivery Policy, Data Processing Addendum and the supporting Trust Centre policies identified below.

1. Overview

This policy describes PCL One's baseline information-security practices for PCL One-managed cloud services and the personnel, systems and service providers used to operate those services. The controls are designed to protect the confidentiality, integrity and availability of customer data and to support secure, resilient service delivery.

POLICY STATUS

This is a public baseline policy. The applicable agreement, Ordering Document, service schedule, data-protection terms and technical design define the service actually purchased and may establish more specific or stricter requirements.

PCL One applies a risk-based security model. Controls are selected according to the service architecture, data handled, customer requirements and applicable contractual or legal obligations. No public policy should be read as disclosing sensitive configuration details that could reduce the effectiveness of a security control.

2. Scope and applicability

Applies to PCL One-managed production services, supporting non-production environments where customer data is present, administrative support processes, monitoring and recovery systems, and approved third parties used to deliver the service.

Customer-managed identity providers, endpoints, networks, integrations, third-party repositories and systems outside the PCL One-managed service boundary remain subject to the controls of their respective owners unless the applicable service design expressly states otherwise.

Relationship to customer agreements

Where an applicable agreement, Ordering Document, service schedule, data-protection term or approved customer security requirement differs from this public baseline, the customer-specific contractual requirement governs for that service.

3. Definitions

Term	Meaning
Customer Data	Data submitted to, stored in, generated by or processed through the subscribed service on the customer's behalf.
Privileged Access	Administrative access capable of changing security-relevant configuration or accessing data beyond ordinary end-user permissions.
Security Event	An observed occurrence that may affect the confidentiality, integrity or availability of an information system or customer data.
Production Environment	The in-scope environment used to provide live customer service.
Service Provider	An approved third party that supports delivery or operation of a PCL One service.
Security Control	An administrative, technical or operational safeguard used to reduce identified information-security risk.

4. Security governance and risk management

PCL One maintains documented security responsibilities and operational controls for the services it manages. Security requirements are considered during service design, customer onboarding, change activity, support, incident response, third-party selection and service exit.

Control area	Public baseline
Governance	Security responsibilities are assigned and material security risks are reviewed through documented operational processes.
Access	Named identities, role-based access, least privilege and strong authentication are used for administrative access.
Data protection	Customer data is protected through access controls, encryption mechanisms and retention/disposal controls appropriate to the service design.
Operations	Security-relevant activity, service health and material operational events are logged or monitored where technically applicable.
Incident response	Security events are triaged, contained, investigated and communicated under the Security Incident & Breach Notification Policy.
Resilience	Backups, recovery procedures and recovery testing support continuity of in-scope services.
Third parties	Providers are assessed according to their role and are subject to security, confidentiality and data-protection obligations appropriate to the service.
Assurance	PCL One maintains supporting control evidence; detailed evidence may be provided through controlled due diligence.

Security controls and supporting procedures are reviewed when there is a material change to the service, risk profile, legal requirement or operating model. Personnel and approved service providers are subject to confidentiality and security obligations appropriate to their roles.

5. Identity and access management

- Administrative access uses named identities rather than shared generic credentials wherever the architecture supports that model.
- Role-based access and least-privilege principles limit privileges to the environment, task and data scope required for the authorized activity.
- Multi-factor authentication is required for PCL One administrative access to in-scope managed environments.
- Privileged elevation is time-bound where supported, and material administrative activity is logged and reviewable.
- Emergency or break-glass access is treated as an exceptional control path and is governed by the Privileged Support & Emergency Access Policy.
- Customer-controlled application roles, approvers and identity-provider configurations remain subject to the applicable service design and customer responsibilities.

6. Data protection and cryptography

PCL One applies technical and operational safeguards to protect customer data throughout the service lifecycle. Service-specific cryptographic implementation may vary by hosting platform and subscribed architecture.

Area	Baseline treatment
Data in transit	Supported external connections to PCL One-managed municipal cloud services use TLS 1.2 or higher, or an equivalent approved secure transport mechanism.
Data at rest	PCL One-managed municipal cloud storage uses AES-256 encryption or the approved encryption mechanism of the applicable cloud platform.
Secrets and keys	Administrative secrets, credentials and cryptographic material are access-restricted according to role and operational need.
Retention and disposal	Customer data, backups and service records follow the applicable retention schedule, legal holds, transition requirements and secure-disposal process.
Residency	Customer-specific data-location and residency commitments are documented in the Ordering Document, service schedule or technical design.
Data minimization	Collection and exposure of unnecessary personal or sensitive data are limited where supported by the business process and service design.

Detailed key-management architecture, credential locations, infrastructure identifiers and other information that could weaken security controls are not included in this public policy.

7. Infrastructure, application and change security

- Production and non-production environments are logically separated according to the service architecture and customer data is segregated from other customers through application, database, tenant or infrastructure controls as applicable.
- Physical data-centre protections are inherited from approved cloud or hosting providers where PCL One uses third-party infrastructure.
- PCL One-managed components are configured and maintained using controlled administrative access and documented operational procedures.
- Security patches, configuration changes and software releases are evaluated and applied according to risk, service impact and the applicable maintenance or release process.
- Production changes are authorized and tested to a level appropriate to their risk before release, except where emergency action is necessary to contain an active security or availability threat.
- Customer data used in non-production environments remains subject to the security and privacy controls applicable to that environment and service design.

Change and maintenance communication

Planned maintenance and customer-impacting changes are communicated in accordance with the Cloud Hosting & Delivery Policy, Ordering Document or service-specific release process. Emergency security work may be performed on an accelerated basis where delay would create material risk.

8. Logging, monitoring and incident management

PCL One maintains logs and monitoring appropriate to the managed service. The purpose of monitoring is to identify service degradation, unauthorized or anomalous activity, backup or integration failures, certificate and dependency issues, and other conditions that may require operational or security response.

Control	Baseline approach
Administrative logging	Administrative and security-relevant activity is logged where supported by the service architecture.
Service monitoring	Service health, integrations, queues, certificates, backup outcomes and security events are monitored for PCL One-managed components.
Triage and escalation	Events are assessed for severity, customer impact, containment needs and escalation to security, operations or service-provider teams.
Evidence preservation	Relevant logs and records are preserved when necessary for investigation, contractual obligations or legal hold.
Customer notification	Confirmed breaches and material customer-impacting incidents are communicated under the Security Incident & Breach Notification Policy and any stricter contractual or legal requirement.

INCIDENT NOTIFICATION

The Security Incident & Breach Notification Policy establishes the public notification baseline. A confirmed breach affecting customer data has a target notification of within 12 hours of confirmation, subject to the conditions and definitions in that policy.

9. Vulnerability management and security testing

PCL One uses a risk-based approach to identify and address vulnerabilities affecting PCL One-managed components. Inputs may include provider security advisories, operational monitoring, defect reports, dependency or configuration review, automated scanning where implemented, and independent assurance or testing activities.

- Material vulnerabilities are evaluated according to exploitability, exposure, affected data, service criticality and available mitigations.
- Remediation may include patching, configuration change, compensating control, provider escalation, feature restriction or service-design change.
- Critical security maintenance may be expedited when normal change timing would create unacceptable risk.
- Detailed vulnerability findings, penetration-test results and remediation evidence are restricted assurance materials and are not published in this policy.

10. Resilience, backup and recovery

Information security includes maintaining the availability and recoverability of in-scope services. PCL One uses backup, monitoring, recovery procedures and periodic exercises appropriate to the subscribed architecture.

Area	Baseline approach
Backups	Automated backups are encrypted and access-controlled, with recovery windows documented for the applicable service.
Restore validation	Restore testing is performed periodically to validate recoverability rather than relying only on backup-success status.
Recovery procedures	Documented recovery runbooks or controlled restoration/failover procedures are maintained for in-scope managed services.
Recovery exercises	Recovery or disaster-recovery exercises are performed periodically, with measured outcomes and corrective actions where needed.
Customer-specific objectives	Availability, RTO, RPO, residency and service-credit terms are governed by the applicable SLA and Ordering Document.

The Service Resilience & Recovery Policy and Cloud Service Availability SLA provide the applicable public baseline objectives. Recovery objectives apply to declared recovery scenarios and are not equivalent to support-case resolution commitments.

11. Third-party and subprocessor security

PCL One may use approved third-party service providers to host, operate or support components of the service. Provider applicability varies by architecture, product, geography and enabled features.

- Security, privacy, confidentiality and service-dependency risks are considered before a provider is used for customer processing.
- Written contractual safeguards are flowed down according to the provider role and sensitivity of the data involved.
- Provider access to customer data is limited to the minimum necessary and is subject to appropriate identity, confidentiality and security controls.
- Material provider changes are handled under the notice and objection process, if any, established by the applicable data-protection terms.
- The public Subprocessor & Third-Party Services Policy is not a substitute for the customer-specific schedule identifying the providers that actually process customer data for the subscribed service.

12. Customer responsibilities

- Maintain accurate authorized-user, administrator, approver and escalation-contact information.
- Configure and protect customer-managed identity providers, endpoints, networks, integrations, credentials and third-party systems according to the agreed design.
- Apply appropriate role assignments and promptly remove access when personnel or business responsibilities change.
- Classify customer data and identify residency, retention, legal-hold, regulatory or evidentiary requirements that affect service design or operation.
- Use supported secure integration methods and avoid introducing unnecessary sensitive data into logs, telemetry or support material.
- Notify PCL One promptly of suspected security events, compromised credentials or material customer-side changes that may affect the service.

13. Exceptions and exclusions

- Controls may vary where the service architecture does not support a particular mechanism; equivalent or compensating controls may be used where appropriate.
- Customer-managed systems, third-party repositories and integrations outside the PCL One-managed service boundary are governed by the controls of those environments.
- Legacy, migration, staging or temporary environments may have different technical characteristics; their permitted use and control treatment are documented where material.
- Security measures may be modified temporarily to contain or recover from an active security incident, provided that the change is controlled, documented and reviewed.
- Detailed infrastructure diagrams, vulnerability findings, account identifiers, detection logic and sensitive assurance evidence are intentionally excluded from this public policy.

14. Assurance and evidence

PCL One maintains records supporting the operation of these security practices. The exact evidence available depends on the service, control scope and customer entitlement.

Evidence area	Examples
Identity and access	Privileged-account inventory, MFA configuration, access grants and expiry records, access-review evidence.
Operations	Change records, security-relevant logs, monitoring records, backup success and restore-test evidence.
Incident response	Incident records, containment and investigation evidence, notification records and corrective actions where applicable.
Resilience	Recovery-exercise results, measured outcomes and tracked corrective actions.
Third parties	Provider due diligence, risk assessment, contractual security terms and relevant provider assurance where available.
Independent assurance	SOC 2 Type 2 report and other restricted-use assurance evidence within the scope of the applicable assessment.

ASSURANCE ACCESS

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.

15. Statement of changes

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