TRUST CENTRE

Acceptable Use Policy

AUTHORIZED USE, PROHIBITED ACTIVITIES, SERVICE PROTECTION AND ENFORCEMENT

Effective Date: 6 October 2025
Classification: Public
Document ID: PCL-TRUST-AUP-006

This document is intended for public distribution. It describes the baseline rules for lawful, secure and responsible use of PCL One cloud services. Product-specific limits, approved security testing arrangements, customer-specific restrictions and enforcement procedures may be governed by the applicable Agreement, Ordering Document, Service Schedule or other service documentation.

Contents

This policy should be read together with the PCL One Cloud Services Agreement, applicable Ordering Document and Service Description, Cloud Hosting & Delivery Policy, Cloud Support Policy, Information Security Practices, Vulnerability Management & Disclosure Policy, Data Processing Addendum and other applicable Trust Centre policies.

1. Overview

PCL One provides cloud services for legitimate business and public-sector operations. This Acceptable Use Policy establishes baseline requirements intended to protect customers, users, PCL One, service providers and the integrity, availability and security of the Services.

> **Public baseline**
> Use of the Services must be lawful, authorized, consistent with the contracted business purpose and conducted in a manner that does not compromise security, privacy, service availability or the rights of others. Customer-specific or service-specific restrictions may be stated in the applicable Order, Service Schedule or Service Description.

2. Scope and contractual relationship

This policy applies to Customers and Users who access or use PCL One cloud services, portals, APIs, integrations, support channels and other PCL One-controlled service interfaces where this policy is incorporated into the applicable contract or Service Specifications.

- The Customer is responsible for its Users and for use of the Services through Customer-controlled accounts, credentials, integrations and systems.
- Where an applicable Agreement, Order, Service Schedule or mandatory law contains a more specific requirement, that requirement controls for the relevant service or activity.
- This policy does not expand a Customer's licensed quantities, subscription scope, data rights or authorized service purpose.

3. Authorized use

Customers and Users may use the Services only within the rights and quantities granted under the applicable contract and for the business, government or organizational purposes for which the Services were ordered.

- Use only supported access methods, documented interfaces and approved integrations unless PCL One has authorized another method.
- Comply with applicable laws, regulatory obligations, third-party rights and Customer policies governing the Customer's own use of the Services.
- Process only data categories and workloads permitted by the applicable Order, DPA, Service Description and documented configuration.
- Cooperate with reasonable service-protection measures, technical limits and security controls that are part of the contracted service design.

4. User and account responsibilities

Customers are responsible for administering their Users and protecting Customer-controlled credentials and access paths. PCL One may provide identity, SSO, MFA or role-based controls, but the Customer remains responsible for assigning appropriate access within its administrative control.

- Use individual named accounts where supported and do not intentionally share credentials in a manner that defeats accountability or access controls.
- Promptly remove or restrict access when a User no longer requires it or when compromise is suspected.
- Do not attempt to bypass MFA, role restrictions, session controls, usage limits or other security safeguards.
- Promptly report suspected unauthorized access, credential compromise or misuse through the designated support or security channel.

5. Unlawful, harmful and abusive conduct

The Services must not be used to conduct, facilitate or materially support activity that is unlawful or that knowingly infringes the rights or safety of others. Prohibited activity includes:

- Fraud, deception, theft, unlawful surveillance, extortion or other illegal activity.
- Content or conduct that is knowingly defamatory, threatening, harassing, abusive or unlawfully discriminatory.
- Infringement or misappropriation of intellectual property, confidentiality, privacy or data-protection rights.
- Distribution of unlawful content or use of the Services to facilitate activity prohibited by applicable law, court order or binding regulatory requirement.
- Use of the Services in violation of applicable export-control, sanctions or trade-restriction requirements.

6. Security interference and malicious activity

Customers and Users must not use the Services to attack, disrupt, compromise or gain unauthorized access to any system, account, service, network, device or data, whether operated by PCL One, another customer, a provider or a third party.

Prohibited activity	Examples
Malicious code	Introducing or distributing malware, ransomware, destructive code, worms, trojans, credential stealers or other harmful software.
Unauthorized access	Credential attacks, account takeover, privilege escalation, exploitation or access beyond the permissions granted to the User.
Service disruption	Denial-of-service activity, deliberate traffic amplification, resource exhaustion or actions intended to degrade availability or performance.
Evasion	Disabling, bypassing or materially interfering with security monitoring, audit logging, rate controls, access restrictions or service-protection mechanisms.

7. Testing, scanning and circumvention

Security testing that could affect the Services or other customers requires prior authorization where such testing is not expressly permitted by the applicable Vulnerability Management & Disclosure Policy or other written PCL One testing rules.

- Do not perform unauthorized vulnerability scanning, port or service discovery, password cracking, exploitation, penetration testing or remote-access testing against PCL One-controlled environments.
- Do not conduct automated load, stress or performance testing that could reasonably affect service stability without prior coordination where required by the applicable service documentation.
- Do not reverse engineer, decompile, disassemble or attempt to derive protected service source code except to the extent a restriction is prohibited by applicable law.
- Security researchers and Customers must use the coordinated reporting process described in the Vulnerability Management & Disclosure Policy and avoid public disclosure that could increase active risk before remediation or coordinated release.

8. Messaging, content and communications

Where a PCL One service includes email, notification, messaging, document exchange or other outbound communication capabilities, Customers are responsible for the legality and appropriateness of the communications they initiate.

- Do not use the Services to send unlawful unsolicited bulk communications, phishing messages, deceptive notices or communications designed to obtain credentials or sensitive information improperly.
- Honor legally required opt-out, consent and communications-preference obligations that apply to Customer-initiated messages.
- Do not impersonate another person or organization in a misleading or unlawful manner, or falsify routing or origin information to conceal abusive activity.
- PCL One may apply technical controls intended to protect deliverability, service integrity and provider reputation where messaging capabilities are used.

9. Resource consumption and service integrity

The Services must be used in a manner consistent with the subscribed service, documented capacity and intended workload. Use that materially threatens platform stability, other customers or provider infrastructure may be restricted even when the activity is not independently unlawful.

- Do not deliberately generate excessive traffic, requests, storage consumption or computational load for the purpose of degrading or evading service controls.
- Do not use the Services for cryptocurrency mining or similarly resource-intensive computation unrelated to the contracted service purpose unless expressly authorized in writing.
- Do not circumvent documented quotas, subscription metrics, rate limits, technical safeguards or capacity controls.

- Where unusual activity is caused by a legitimate business event, Customers should coordinate with PCL One when service documentation or support guidance requires advance planning.

10. Data, privacy and intellectual property

Customers retain responsibility for ensuring they have the rights and lawful basis needed to provide Customer Data to the Services and to instruct PCL One to process it under the applicable Agreement and DPA.

- Do not upload data that the applicable Order, Service Description or DPA expressly excludes from the subscribed service.
- Do not use the Services to obtain, disclose or expose personal information, confidential information or protected records without appropriate authorization.
- Do not use third-party content, software, datasets, trademarks or other materials in a manner that infringes applicable rights or license conditions.
- Customer Data handling, retention, deletion, residency and subprocessor terms are governed by the applicable DPA and Trust Centre policies rather than by this Acceptable Use Policy alone.

11. Integrations, automation and APIs

Customers may use supported APIs, connectors and automation capabilities within the permissions, limits and purposes made available for the subscribed service.

- Automation must authenticate through supported mechanisms and must not be used to evade access, rate, logging or usage controls.
- Customers are responsible for credentials and systems they connect to the Services and for the lawful transfer of data through Customer-directed integrations.
- Unsupported scraping, extraction or automated interaction that materially affects service operation or bypasses documented interfaces may be restricted.
- PCL One may require changes to a Customer integration when necessary to address material security, stability, compatibility or provider requirements.

12. AI-enabled features

Where a subscribed service includes AI-assisted capabilities, Customers remain responsible for how they configure and use those capabilities, the inputs they provide, and decisions made using outputs. Feature-specific AI terms, service descriptions and data-protection commitments may impose additional requirements.

- Do not use AI-enabled features to bypass restrictions that apply to the underlying Service or to process data categories prohibited by the applicable service terms.
- Users should apply appropriate human review where an AI-assisted output is used for a decision that could materially affect an individual, financial record, legal obligation or public-sector process.
- Use of AI-enabled features does not transfer responsibility for Customer instructions, lawful basis, accuracy review or required approvals to PCL One.

13. Monitoring, investigation and cooperation

PCL One may use security, operational and abuse-detection controls to protect the Services and investigate suspected violations, subject to the Agreement, DPA and applicable law. Such controls may include review of logs, metadata, technical indicators, support information and other evidence reasonably necessary to understand the activity.

- Customers must reasonably cooperate with investigation of suspected compromise, abuse or activity originating from Customer-controlled accounts or integrations.
- PCL One seeks to limit investigative access to information reasonably necessary for security, service integrity, legal compliance or contract enforcement.
- Where a matter also constitutes a security incident or Personal Data Breach, the applicable Security Incident & Breach Notification Policy and DPA govern incident handling and notification.

14. Remedial action, suspension and restoration

If PCL One reasonably determines that use of the Services violates this policy or creates a material security, legal or availability risk, PCL One may take proportionate remedial action consistent with the governing Agreement and applicable law.

Circumstance	Possible response
Lower-risk or correctable misuse	Contact the Customer, request corrective action, apply technical guidance or require configuration changes.
Material service or security risk	Restrict affected functionality, credentials, traffic, integration paths or access to the extent reasonably necessary to contain the risk.
Urgent threat or legal requirement	Take immediate protective action where delay would materially increase harm, including temporary suspension or isolation of affected access.
Resolution	Restore affected access when the material risk has been addressed, subject to the Agreement, technical feasibility and any continuing legal restriction.

Proportionate enforcement

PCL One seeks to use the least disruptive action reasonably available for the circumstances. Advance notice may not be possible where immediate action is required to protect security, service availability, another customer, a third party or compliance with law.

15. Reporting suspected misuse

Customers should promptly report suspected abuse, unauthorized use, credential compromise, malicious activity or other apparent violations through the applicable PCL One support or security reporting channel identified in the service documentation or customer support materials.

- Reports should include available timestamps, affected accounts or services, observed behavior and relevant technical details without unnecessarily exposing sensitive information.
- Security vulnerabilities should be reported through the coordinated process described in the Vulnerability Management & Disclosure Policy.
- Reports submitted in good faith are evaluated according to the nature and urgency of the issue; reporting a concern does not by itself establish that a violation occurred.

16. Related documents and exceptions

Document	Relationship
PCL One Cloud Services Agreement	Contractual rights, use restrictions, suspension and general Customer obligations.
PCL One Cloud Hosting & Delivery Policy	Service operation, protection, monitoring and hosting controls.
PCL One Information Security Practices	Security governance, access control, logging and operational safeguards.
PCL One Vulnerability Management & Disclosure Policy	Authorized vulnerability reporting, coordinated testing and disclosure.
PCL One Data Processing Addendum	Processing instructions, privacy obligations and personal-data protections.
PCL One Cloud Support Policy	Support channels, case handling and escalation for service issues.

Any approved exception to this policy must be documented through the applicable contractual, security or service-governance process. An exception for one Customer, service or activity does not create a general waiver for other uses.

17. Statement of changes

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