Cloud Use and Support Policy

SKNK Cloud

Version 3.0 | 24 October 2026

1. Provider, scope and related documents

SHIKANOKO NETWORKS LTD, registered in England and Wales under company number 17131877, with its registered office at 128 City Road, London, United Kingdom, EC1V 2NX, operates SKNK Cloud. General contact: admin@shikanoko-networks.com.

This policy sets common rules for the Cloud website, configuration tools, enquiries and, where expressly incorporated into an accepted order, Cloud services. The applicable product description, product agreement, order and service schedules determine each customer's configuration, capacity, permitted usage, support and service levels. This policy does not set a single bandwidth, traffic allowance, price or response time for every product.

Read it with the Cloud Terms of Service at /cloud/terms, the Cloud Privacy Notice at /cloud/privacy and the AUP version identified for your service. Mandatory law and the contractual order of precedence govern any conflict. This policy does not amend an existing ASN sponsorship, IPv4 or other agreement, or enable ordering, payment or activation.

2. Lawful use and authority

Use the website and service lawfully, within the scope and permissions granted to you. You are responsible for content you provide, instructions you issue and people you authorise to use your service. Obtain the permissions needed for third-party data, intellectual property and Internet number resources. Do not misrepresent your identity, authority or another person's approval.

Do not use the service for unlawful content or activity; phishing, fraud or impersonation; malware or unauthorised access; denial-of-service attacks or deliberate network disruption; spam or abusive messaging; unauthorised interception; or infringement of another person's lawful rights. Security research or testing that could affect our or another person's systems requires the relevant authorisation in advance. Lawful security tools and ordinary high usage are not violations merely because of their name or volume; the agreed limits, authorisation, effects and applicable law matter.

Keep credentials, private keys, payment details and unnecessary personal information out of configuration URLs and public reports. A configuration selection, support reply or product label does not authorise a use outside the accepted service scope.

3. Network and resource use

Where a service includes routing or Internet number resources, use only resources you control or are authorised to use and announce. Provide proportionate evidence of authority when reasonably requested and keep relevant authorisation and routing records accurate. Do not hijack routes, forge authorisations or deliberately announce unauthorised prefixes or create harmful route leaks.

We may apply proportionate filters and safeguards for network security, resource authority and agreed service limits. Session counts, prefix scope, address use, traffic measurement and excess-use handling are product-specific and must be disclosed in the applicable service documents. A port or speed description is not an additional dedicated-bandwidth guarantee. Paid additions or overage require the agreement specified in the Cloud Terms; this policy creates no extra charge.

4. Customer and provider responsibilities

The accepted service documents allocate infrastructure, operating-system, application, content, routing, security and backup tasks. For an unmanaged service, you perform the management tasks assigned to you and maintain independent copies of data you cannot afford to lose. We remain responsible for the infrastructure and functions assigned to us, our authorised personnel, applicable security duties and our own contractual breaches.

A general support exclusion does not remove an expressly included task or a mandatory remedy. We access customer content only where authorised and reasonably necessary for the agreed service, documented instructions, security response or law. This policy does not impose a general monitoring obligation beyond applicable law and the accepted service, grant unlimited access to customer data, or include a managed backup merely because storage is allocated.

5. Support and reporting channels

Send general questions, service issues, billing queries, complaints and review requests to admin@shikanoko-networks.com. Send resource-authority and routing matters to noc@shikanoko-networks.com, and abuse or illegal-content reports to abuse@shikanoko-networks.com. Identify the relevant service or page, the time and time zone, the observed issue and enough non-sensitive detail for us to investigate. An order or decision reference is helpful where available.

Support scope, service hours, severity handling and any contractual service level are specified for the purchased service. A contact address does not create continuous staffing, an uptime guarantee or a fixed response, resolution or recovery time. We will handle matters diligently and with the care and skill required by applicable law, and comply with any specific response duty that applies. An enquiry does not reserve capacity or form an order.

Do not send passwords, private keys, authentication codes, full payment-card numbers or unnecessary identity documents. If an investigation needs sensitive evidence, ask for an appropriate protected channel. Do not reproduce illegal material unnecessarily; provide its precise location and a description instead.

6. Maintenance, incidents and cooperation

We may perform maintenance and apply proportionate security or network-protection measures. We provide notice where reasonably practicable and meaningful updates for material incidents as required by the applicable service commitment or law. Urgent containment may have to precede notice. Planned maintenance does not by itself remove an agreed service obligation or statutory remedy.

Notify us promptly of suspected compromise or harmful use affecting your service. Cooperate with reasonable, proportionate requests needed to investigate, contain and remedy the incident. We distinguish provider-controlled faults from customer-managed tasks rather than treating every incident as outside support. Recovery work, changes or extra paid assistance outside the purchased scope require a clear agreement before charges arise, subject to any duty to remedy our own breach.

7. Illegal-content notices

Where the applicable Digital Services Act hosting rules require it, our electronic notice-and-action channel accepts sufficiently precise and substantiated illegal-content notices at abuse@shikanoko-networks.com. A notice should include the precise electronic location and necessary technical identifier, an explanation of why the content is illegal, the reporter’s name and email where legally required, and a statement of good faith that the information is accurate and complete. The legally permitted exception for identifying details in specified child-sexual-abuse reports is respected.

We acknowledge receipt and give the reporter the decision and available redress without undue delay where required. We examine notices in a timely, diligent, non-arbitrary and objective manner, considering the content, context and applicable law. A report is not automatic proof of illegality. Any use of automated tools in handling or deciding notices is disclosed as required, and relevant contested findings are available for human assessment.

This channel concerns material hosted through a service to which the relevant duties apply. Ordinary product questions belong with general support. These rules do not claim that a public information website or every VPS use is an online platform, or that a support inbox replaces a platform-specific statutory complaints system.

8. Restrictions and statements of reasons

We may restrict affected content, routes, access or service only on a lawful contractual or legal basis, including material breach, non-payment after notice and a reasonable remedy opportunity, a binding legal requirement or an urgent security or abuse risk. Where practicable we first give notice and allow explanation or remedy. Immediate action may be needed for urgent containment or where law prevents notice.

We choose a proportionate measure, limit it to affected functions where feasible, and reassess it when the risk or facts change. A report or complaint alone does not justify unrelated service termination. Any fee, refund, termination and data-retrieval consequences follow the accepted contract and mandatory law; this policy does not create a blanket forfeiture or immediate-erasure right.

Where law requires a statement of reasons for a restriction based on illegal content or incompatibility with our terms, we provide it no later than the restriction takes effect, subject to statutory exceptions. It identifies the measure, scope and duration, relevant facts, whether a notice or our investigation triggered it, any

relevant automated means, the legal or contractual basis and available redress. We protect confidential information and comply with lawful restrictions on disclosure without using them as a general excuse to withhold reasons.

9. Review, complaints and remedies

Request review through admin@shikanoko-networks.com, identifying the decision or affected service and your reasons, with relevant evidence that you are entitled to provide. We assess the matter fairly, consider relevant new information and correct an unjustified restriction. Where an applicable law sets specific acknowledgement, response, review or complaint procedures, we follow them.

This review does not waive your rights to a competent regulator, statutory complaint mechanism, available certified out-of-court process or court. It does not limit consumer withdrawal, refund or service-conformity rights, nor mandatory data-protection, switching or retrieval rights. Our support process does not replace the particular procedure required by a law simply because you used this contact address.

10. DSA representative and separate privacy requests

For matters within the Digital Services Act representative appointment for SHIKANOKO NETWORKS LTD, trading as SKNK / SKNK Cloud / IPIP.one, contact DataRep at digitalrequest@datarep.com. The DSA postal contact is DataRep, 77 Camden Street Lower, Dublin, D02 XE80, Republic of Ireland. Identify the company and relevant service; current representative details are also maintained at /privacy#dsa-representative.

Data-protection requests use admin@shikanoko-networks.com directly or DataRep’s separate data-protection channel, datarequest@datarep.com and https://www.datarep.com/data-request, as described in the privacy notice. A representative appointment does not transfer our own obligations, establish a DPO appointment, or certify all Cloud operations as compliant. You do not have to contact DataRep before contacting us or an authority.

11. Versions and changes

This policy is version 3.0, dated 24 October 2026. Website-use provisions apply from publication; service provisions apply only where incorporated into the accepted service contract. We may publish updates for future use and will give material-change information as required by law.

A later webpage does not retrospectively change an accepted order, increase a charge, remove an agreed remedy or expand suspension authority. Changes to an existing service require its lawful change mechanism, a valid agreement or mandatory law. English is the contract language unless expressly agreed otherwise; the full Chinese translation is for convenience and cannot reduce mandatory consumer or language rights.