

SERVICE SPECIFIC TERMS / SECURITY

Secure Access and Security Service Edge

Powered by Netskope

VERSION
v2026.10cEFFECTIVE
1 November 2026

These Service Specific Terms form part of your agreement with FirstNet Technology Services (Pty) Ltd. Read them with the FirstNet Standard Terms and Conditions (or your signed Master Services Agreement), your Service Schedule and the Data Processing Annexure, all available at www.firstnet.co.za/legal-notices/.

1. Status and precedence

- 1.1 These Service Specific Terms ("SST") apply to the Netskope-based secure access and Security Service Edge (SSE) Services that FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07) ("FirstNet") provides to the Customer, whether as licence supply, deployment, co-management or a managed service.
- 1.2 These SST form part of the agreement between FirstNet and the Customer, which is either the FirstNet Standard Terms and Conditions or the Customer's signed Master Services Agreement with FirstNet (the "Agreement"). They are incorporated into the Agreement by reference and are published at www.firstnet.co.za/legal-notices/.
- 1.3 The Netskope modules, number of users, service model, responsibility split, reporting cadence, MRC, NRC and Initial Period are set out in the Service Schedule, quote or scope of work accepted by the Customer (the "Service Schedule").
- 1.4 If documents conflict, they apply in this order: (a) the Service Schedule, but only for commercial items it expressly overrides; (b) these SST; (c) the Agreement (including the Data Processing Annexure and the Acceptable Use Policy); (d) the Vendor Terms. Where the Vendor Terms impose a mandatory restriction on how the Vendor's product may be used, the Customer must comply with that restriction.
- 1.5 Words defined in the Agreement have the same meaning in these SST.

2. Definitions

- 2.1 **"Inspection"** means the inline examination by the Netskope platform of the Customer's users' internet, cloud application and private application traffic, including decryption of TLS-encrypted traffic, and the scanning of content for data loss prevention.
- 2.2 **"Netskope Client"** means the Netskope software agent installed on users' devices to steer traffic to the Netskope platform.
- 2.3 **"Policy"** means the web, cloud application, data protection, access and isolation rules configured on the Netskope platform for the Customer.
- 2.4 **"Proof of Value"** means a time-limited trial of a Netskope use case with a small group of users against agreed success criteria.
- 2.5 **"Service Model"** means the model stated in the Service Schedule: Supply (licences only), Deploy (design and set-up, then handover), Co-manage (shared operation) or Managed service (FirstNet operates the platform within an agreed scope).

3. Service description

- 3.1 Platform. Netskope provides the Netskope One cloud platform, which may include, as stated in the Service Schedule: Secure Web Gateway (SWG); Cloud Access Security Broker (CASB); Data Loss Prevention (DLP) across web, SaaS, endpoint, email and AI channels; Private Access (zero trust network access); Remote Browser Isolation (RBI); and Advanced Analytics. Traffic is carried over Netskope's NewEdge network.
- 3.2 What FirstNet provides, by Service Model.
 - 3.2.1 Supply: FirstNet supplies Netskope licences for the agreed use case. The Customer or its chosen partner deploys and operates the platform. FirstNet provides licensing support and escalation to Netskope.
 - 3.2.2 Deploy: FirstNet designs and sets up the platform (admin access, identity integration, traffic steering, Inspection rules and exceptions, first Policies, reporting), runs a pilot and hands the platform over with documented Policies.
 - 3.2.3 Co-manage: as Deploy, then FirstNet and the Customer share Policy tuning, alert review and reporting, as divided in the Service Schedule.
 - 3.2.4 Managed service: as Deploy, then FirstNet operates the platform within the scope, change allowance and reporting cadence in the Service Schedule.
- 3.3 Responsibility split. The Service Schedule records who owns each activity after go-live (for example Policy changes, DLP alert review, user onboarding, Netskope Client deployment). Where the Service Schedule is silent, the Customer owns the activity.
- 3.4 Proof of Value. A Proof of Value is provided for evaluation only, for the period agreed in writing, "as is", without service levels, and may be ended by either party at any time. Data from a Proof of Value may be deleted when it ends.
- 3.5 What is not included. Unless the Service Schedule says otherwise, the Service does not include: deployment of the Netskope Client to devices (which the Customer does through its device management tools, with FirstNet's guidance); remediation of SaaS misconfigurations or data incidents that the platform finds; investigation of employee conduct; SD-WAN or networking (SASE networking is a separate Service); managed detection and response; or any guarantee of a compliance outcome.

4. Vendor Terms

- 4.1 The Service uses Netskope's services, which are subject to the following Vendor Terms. The Customer accepts them when it orders or first uses the Service:
 - 4.1.1 Netskope Subscription Services Agreement (<https://www.netskope.com/subscription-terms>);
 - 4.1.2 Netskope Software EULA for the Netskope Client (<https://www.netskope.com/software-eula>); and
 - 4.1.3 Netskope Privacy Policy (<https://www.netskope.com/privacy-policy>) and the Netskope customer data processing addendum, as provided or linked by FirstNet.
- 4.2 Netskope's Subscription Services Agreement applies to subscriptions bought through a reseller. FirstNet may not change it or make promises on Netskope's behalf.
- 4.3 Netskope may change its services, modules and Vendor Terms. FirstNet is not liable for those changes. Where a change materially affects the Service, FirstNet will tell the Customer and the change provisions of the Agreement apply.
- 4.4 Netskope may suspend the Service for breach of its terms. FirstNet is not liable for that suspension.
- 4.5 FirstNet passes through Netskope's warranties and service levels only to the extent it is allowed to and does not add its own.

5. Customer responsibilities

- 5.1 Identity and devices. The Customer must provide and maintain its identity provider integration (SAML or OIDC, user groups and multi-factor authentication) and deploy and maintain the Netskope Client on in-scope devices.

- 5.2 Licence counts. The Customer must keep the number of users or devices within the licensed quantity and tell FirstNet promptly of growth.
- 5.3 Policy decisions. The Customer decides what traffic is inspected, decrypted, blocked, isolated or allowed, which data types DLP looks for, which applications users may reach, and which categories are excluded from Inspection. FirstNet advises and configures on the Customer's written instructions or approved Change Requests. The Customer is responsible for the effect of Policies it approves on its users and business.
- 5.4 Notices and consents (traffic inspection). Before Inspection starts for any user, the Customer must:
 - 5.4.1 have a lawful basis under POPIA for processing its users' personal information through the Service, and give them notice of the processing under section 18 of POPIA, including that traffic and data may be processed outside South Africa;
 - 5.4.2 inform its users in advance, in writing, that their communications on the Customer's systems may be intercepted and monitored, and obtain any consents needed, so that the Inspection is lawful under section 6 (or, where relevant, section 5) of RICA;
 - 5.4.3 put in place the workplace policies (for example an acceptable use, monitoring or bring-your-own-device policy) and, where required, consultation with employees or their representatives that apply to it under labour law; and
 - 5.4.4 configure (or instruct FirstNet to configure) appropriate exclusions from TLS decryption, for example for banking, health and legally privileged traffic, and for personal devices where appropriate.
- 5.5 Contractors and third parties. Where the Service covers contractors, guests or other non-employees, the Customer must give them equivalent notices.
- 5.6 Use of findings. The Customer is responsible for how it uses information the Service reveals about individuals, including in disciplinary processes.
- 5.7 The Customer must comply with the Acceptable Use Policy and the Vendor Terms, and must name Technical Contacts authorised to approve Policy changes.

6. Provisioning and lead times

- 6.1 Deployment follows: discovery; optional Proof of Value; admin access, identity integration, traffic steering and first Policies; a pilot with a smaller group of users; production rollout; and handover with documented Policies, reporting and support channels. Lead times are indicative only.
- 6.2 The Service Commencement Date is the date the platform is handed over for production use (Deploy, Co-manage and Managed service) or the date licences are activated (Supply).

7. Service levels and support

- 7.1 Support. The Customer logs incidents and requests through the FirstNet Rapid Response Service Desk as described in the Rapid Response Services Guide published at www.firstnet.co.za/legal-notices/ (currently <https://www.firstnet.co.za/api/media/file/SOP-SVC-RR-001-Rapid-Response-Services-Guide.pdf>). FirstNet escalates platform issues to Netskope.
- 7.2 Service levels. FirstNet's response, change and reporting commitments for Co-manage and Managed service are stated in the Service Schedule; where none is stated, FirstNet uses reasonable endeavours and passes through Netskope's service level. Netskope platform availability is as provided under the Vendor Terms.
- 7.3 Exclusions. Targets do not apply to failures caused by Netskope platform or network outages, the Customer's identity provider, devices or connectivity, Policies the Customer approved or changed, the Customer's failure to deploy or update the Netskope Client, or force majeure.
- 7.4 Service credits apply only if the Service Schedule states them, and they are then the Customer's sole financial remedy for the failure concerned. This does not limit the Customer's right to terminate the affected Service for material or repeated breach under the Agreement.

8. Data, privacy and security

- 8.1 Roles. The Service processes Customer Personal Information, including user identities, device details, browsing and application activity, and the content of files and messages scanned for DLP. FirstNet processes it as the Customer's operator under POPIA and Netskope as FirstNet's sub-operator. The Customer is the responsible party. The Data Processing Annexure published at www.firstnet.co.za/legal-notices/ applies.
- 8.2 FirstNet will process Customer Personal Information only with the Customer's knowledge or authorisation, for the purpose of providing the Service, will treat it as confidential, and will maintain appropriate, reasonable security measures as required by section 19 of POPIA. FirstNet staff will access user activity data only as needed to provide the Service or as the Customer instructs.
- 8.3 Security compromises. If FirstNet has reasonable grounds to believe that Customer Personal Information has been accessed or acquired by an unauthorised person, FirstNet will notify the Customer immediately, as required by section 21(2) of POPIA. The Customer decides on notification under section 22 of POPIA.
- 8.4 Where data is held. FirstNet's own records for the Service are held in South Africa by default. Netskope hosts the Customer's tenant, including logs and event data, in South Africa. Netskope processes each user's traffic at the NewEdge data centre nearest to that user, so traffic of users who are outside South Africa may be processed outside South Africa.
- 8.5 Cross-border transfers. Where Customer Personal Information is processed outside South Africa as described in clause 8.4, the transfer is made only where section 72(1) of POPIA allows it, as set out in clause 7.3 of the Data Processing Annexure. FirstNet relies mainly on Netskope being bound by its data processing addendum as a binding agreement that provides an adequate level of protection (section 72(1)(a)). The Customer must include the transfer in its notices to users under clause 5.4.1.
- 8.6 Exit. Before the Service ends, the Customer may request an export of its Policies and available reports. After the Service ends, Netskope deletes the Customer's tenant data in accordance with the Vendor Terms.

9. Fees, licences and changes

- 9.1 The MRC, NRC and any usage charges are set out in the Service Schedule. These SST do not state prices.
- 9.2 Netskope licences are charged per user or as stated in the Service Schedule. Additional users or modules are charged from the next billing cycle. If actual usage exceeds the licensed quantity, FirstNet may invoice the excess.
- 9.3 Netskope price increases and Charges linked to a foreign currency are dealt with under the Agreement: Vendor price increases may be passed on under clause 9.5 of the Standard Terms and Conditions (without mark-up, with reasonable details and on at least 30 (thirty) calendar days' written notice), and foreign-currency-linked Charges follow the exchange rate and basis stated in the Service Schedule under clause 9.6.
- 9.4 Deployment, migration and work outside the Service Schedule are charged as quoted.

10. Term, cancellation and early termination

- 10.1 The Service runs for the Initial Period in the Service Schedule from the Service Commencement Date, and then continues month to month until either party gives at least 30 (thirty) calendar days' written notice, or 90 (ninety) calendar days' written notice where the Service Schedule states that the upstream provider of the Service requires that period (clause 3.5.2 of the Standard Terms and Conditions).

- 10.2 If the Customer cancels before the end of the Initial Period, the early termination charges in the Agreement apply, unless the Service Schedule states different charges. Netskope subscriptions are committed for the subscription term stated in the Service Schedule and cannot be cancelled during that term. Because FirstNet holds them under its own agreement with Netskope, the Customer may reduce the number of users or modules at any time on written notice, down to the minimum quantity Netskope sets for the subscription (the "Vendor minimum"). If the Customer cancels during the committed term, the Charges for the Netskope subscription at the Vendor minimum for the rest of its committed term remain payable under clause 19.4 of the Standard Terms and Conditions, instead of (not in addition to) the early termination charge for the same component and months; the early termination charge in the Agreement applies only to the other components of the Service. Where the Customer is a Consumer, only a reasonable cancellation penalty may be charged under section 14 of the CPA and regulation 5. FirstNet applies the same reasonable cancellation penalty to a Small Business Customer (clause 19.3 of the Standard Terms and Conditions).
- 10.3 At the end of the Service the Customer must remove the Netskope Client and re-route traffic. Users lose protection and access through Private Access when the subscription ends; the Customer must plan alternative access to private applications before then.

11. Suspension

- 11.1 FirstNet may suspend all or part of the Service, on as much notice as is reasonable in the circumstances, if the Customer does not pay undisputed Charges when due, breaches the Acceptable Use Policy or the Vendor Terms, if Netskope suspends the Service, if the Customer's use creates a security risk, or if the law or a competent authority requires it. Suspension of Private Access may stop users reaching private applications.

12. Liability specifics

- 12.1 The limitations and exclusions of liability in the Agreement apply. These SST do not state a separate cap.
- 12.2 Subject to the Agreement, FirstNet is not liable for loss or damage arising from: threats or data loss that the platform did not detect or prevent where FirstNet provided the Service in accordance with these SST; Policies that block or allow traffic as the Customer approved; the Customer's failure to give the notices or obtain the consents or policies in clause 5.4; the Customer's use of information about individuals that the Service reveals; or activities that the Service Schedule allocates to the Customer.
- 12.3 The Service strengthens control, visibility and reporting but does not on its own guarantee compliance with POPIA or any other law or standard.
- 12.4 Nothing in these SST limits liability that cannot be limited by law.

13. Regulatory notes

- 13.1 RICA and employee monitoring. See clause 5.4. Inspection of communications without the required notice may be an offence under RICA and an interference with privacy under POPIA.
- 13.2 POPIA special personal information. DLP rules may detect special personal information (for example health information) or children's information. The Customer is responsible for confirming that it may process that information for this purpose under sections 26 to 35 of POPIA.
- 13.3 Cybercrimes Act. Where section 54 of the Cybercrimes Act 19 of 2020 applies to FirstNet, FirstNet will report offences and preserve information as required, and may disclose what the law requires.

14. Changes to these terms

- 14.1 FirstNet may update these SST to reflect changes in Netskope's services or Vendor Terms, changes in law, security requirements or changes in how FirstNet provides the Service. FirstNet will give at least 30 (thirty) days' notice of a material change by email or by publishing it at www.firstnet.co.za/legal-notices/. If a material change is to the Customer's material detriment, the Customer may cancel the affected Service by notice before the change takes effect, without an early termination charge, except for a committed Netskope subscription under clause 10.2.
- 14.2 The version number and effective date below identify this version.

Secure Access and Security Service Edge | Version v2026.10c | Effective date: 1 November 2026

Published by FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07), 26 Augrabies Road, Waterfall Office Park, Midrand, 1686 | 0861 989 896 | support@firstnet.co.za

Published by FirstNet Technology Services (Pty) Ltd, registration number 2006/031608/07. Secure Access and Security Service Edge, v2026.10c. The current version of every FirstNet legal document is at www.firstnet.co.za/legal-notices/.