

SERVICE SPECIFIC TERMS / SECURITY

Cloudflare Web, DDoS and Zero Trust

Application security, DDoS protection, Zero Trust and network services, powered by Cloudflare

VERSION
v2026.10c

EFFECTIVE
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 Cloudflare-based Services that FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07) ("FirstNet") provides to the Customer using Cloudflare's services, with FirstNet's managed service around them.
- 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 Cloudflare plan and products, protected domains, applications, users, IP prefixes, managed-service tier, 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 Cloudflare's services 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 **"Cloudflare Account"** means the Customer's own account on the Cloudflare platform, in which the Customer's Cloudflare services are configured (see clause 3.3).
- 2.2 **"Edge Certificate"** means a TLS certificate used by Cloudflare to terminate encrypted connections to the Customer's domains at the Cloudflare edge, whether issued through Cloudflare or uploaded by the Customer.
- 2.3 **"Origin"** means the Customer's servers, applications or networks that Cloudflare protects or connects to.
- 2.4 **"Prefix"** means an IP address range that the Customer asks Cloudflare to advertise and protect using Magic Transit.
- 2.5 **"Protected Asset"** means a domain, application, API, user group, site or Prefix listed in the Service Schedule.

3. Service description

- 3.1 Cloudflare platform. Cloudflare, Inc. operates a global network with points of presence in many countries. The products in scope are those named in the Service Schedule, which may include:
 - 3.1.1 Application Services: Web Application Firewall (WAF), DDoS protection (layers 3, 4 and 7), Bot Management, API Shield, CDN and Argo Smart Routing;
 - 3.1.2 Zero Trust: Cloudflare Access (zero trust network access), Cloudflare Gateway (secure web gateway), Browser Isolation, CASB and DLP; and
 - 3.1.3 Network Services: Magic Transit, Magic WAN and Magic Firewall.

- 3.2 What FirstNet provides (the managed wrap). Within the scope and tier in the Service Schedule, FirstNet:
- 3.2.1 runs discovery and a phased design, aligned with Cloudflare's technical account team where applicable;
 - 3.2.2 sets up the Cloudflare Account with single sign-on, multi-factor authentication, audit logging and role-based access;
 - 3.2.3 onboards Protected Assets (domains and DNS, identity provider integration and application catalogue, or BGP and tunnel topology);
 - 3.2.4 stages the WAF in detection (log) mode first, tunes it against real traffic, and moves to enforcement only after the Customer approves, keeping a documented rollback path until then;
 - 3.2.5 hardens DDoS settings and Zero Trust and Gateway policies;
 - 3.2.6 forwards logs to the Customer's SIEM or FirstNet monitoring where stated in the Service Schedule;
 - 3.2.7 provides ongoing false-positive triage, attack-event reviews and service reviews at the cadence in the Service Schedule; and
 - 3.2.8 acts as the Customer's single point of entry for support, with escalation into Cloudflare.
- 3.3 Account ownership. FirstNet creates a separate Cloudflare Account for each Customer, under the Customer's own account name, within FirstNet's Cloudflare MSSP organisation. FirstNet and the Customer jointly hold the Cloudflare Account, and FirstNet administers it for the Service. The Customer's domains, DNS zones, Prefixes, certificates and configuration remain the Customer's, and on exit FirstNet will hand the Cloudflare Account over to the Customer, or move the zones and configuration, under clause 10.4.
- 3.4 What is not included. Unless the Service Schedule says otherwise, the Service does not include: a security operations centre or managed detection and response service (Cloudflare is a security platform, not a SOC; see the Managed Detection and Response Service Specific Terms); development or changes to the Customer's applications or Origin; penetration or load testing (which Cloudflare's terms prohibit without its written consent); Developer Platform services (Workers, R2, D1); or uptime commitments beyond those stated in the Service Schedule.
- 3.5 Related services. These SST cover Cloudflare services only, including Magic Firewall. Firewalls at the Customer's sites or on FirstNet's hosted firewall platform (Fortinet and Sophos) are covered by the Managed Firewall Service Specific Terms.

4. Vendor Terms

- 4.1 The Service uses Cloudflare's services, which are subject to the Vendor Terms below, depending on the plan in the Service Schedule. The Customer accepts them when it orders or first uses the Service:
- 4.1.1 Enterprise plans: Cloudflare Enterprise Subscription Agreement (<https://www.cloudflare.com/enterpriseterms/>, effective 12 September 2025), including the Service-Specific Terms (<https://www.cloudflare.com/service-specific-terms-overview/>), the Information Security Exhibit (<https://www.cloudflare.com/security-exhibit/>) and the Enterprise Support and SLA (<https://www.cloudflare.com/enterprise-support-sla/>);
 - 4.1.2 Free, Pro and Business (self-serve) plans: Cloudflare Self-Serve Subscription Agreement (<https://www.cloudflare.com/terms/>, last updated 12 September 2025) and the Service-Specific Terms; and
 - 4.1.3 all plans: Cloudflare Data Processing Addendum (<https://www.cloudflare.com/cloudflare-customer-dpa/>, version 6.4) and Cloudflare's approach to abuse (<https://www.cloudflare.com/trust-hub/abuse-approach/>).
- 4.2 Where the Customer buys Cloudflare's services through FirstNet, payment and cancellation are governed by these SST and the Agreement, and any Cloudflare refunds or credits are issued through FirstNet. FirstNet may not change Cloudflare's terms or make commitments on Cloudflare's behalf.
- 4.3 Cloudflare's terms restrict use, including bans on reselling or sublicensing, reverse engineering, sending malicious code, circumventing usage limits, and running penetration or load tests without Cloudflare's written consent. The Customer must not breach those restrictions.

- 4.4 Cloudflare may change its services 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.
- 4.5 Cloudflare may suspend the Service immediately if the Customer's use harms other customers or its network, if needed to comply with law, or for non-payment. FirstNet is not liable for that suspension.
- 4.6 Cloudflare's service level and support (for Enterprise plans) are as set out in the Enterprise Support and SLA, under which service credits are the sole remedy. FirstNet passes through Cloudflare credits it receives for the Customer's account and does not add its own service level for the Cloudflare platform. Where FirstNet's agreement with Cloudflare includes terms that apply to the Customer, they are the Vendor's terms that apply to the Service, as provided or linked by FirstNet.

5. Customer responsibilities

- 5.1 DNS authority. The Customer must own or control the Protected Asset domains and their DNS, and provide proof of ownership on request. The Customer authorises FirstNet to make the DNS and nameserver changes needed for the Service (for example changing nameservers to Cloudflare, or adding CNAME or TXT records), each with the prior approval of a Technical Contact. The Customer remains the registrant and keeps authority over its registrar account.
- 5.2 Prefixes and BGP (Magic Transit). The Customer must hold the right to use each Prefix, provide a letter of authorisation and keep its routing registry and RPKI records accurate as Cloudflare and FirstNet specify, and coordinate BGP changes with its network team and upstream carriers.
- 5.3 Certificates and keys. The Customer chooses whether to use Cloudflare-issued Edge Certificates or upload its own. Where the Customer uploads a certificate and private key, the Customer is responsible for its validity, renewal and revocation and authorises Cloudflare to store and use the private key to terminate TLS for the Protected Asset (unless a keyless option is ordered). The Customer must configure encryption between Cloudflare and its Origin as FirstNet recommends (for example full strict TLS).
- 5.4 Identity (Zero Trust). The Customer must provide and maintain its identity provider integration, user groups, multi-factor authentication and device-posture tools, and an application catalogue with owners.
- 5.5 Origin. The Customer is responsible for its Origin, applications and content, for patching and securing them, and for keeping its own copies of its data and logs (Cloudflare may delete log files after a short period).
- 5.6 Change windows. The Customer must name Technical Contacts, agree change windows and acceptance criteria before cut-over, and approve each move from detection to enforcement.
- 5.7 Lawful use. The Customer must comply with the Acceptable Use Policy and the Vendor Terms, and must not use the Service for unlawful content or activity. The Customer is responsible for the content served through the Service.
- 5.8 Traffic inspection. Gateway, Browser Isolation, CASB and DLP inspect users' traffic and content. The Customer must give its users the notices, and obtain the consents, required by section 6 of RICA, POPIA and labour law before inspection starts, and decide which categories are excluded (see the equivalent duties in the Secure Access and Security Service Edge Service Specific Terms, which apply here with the necessary changes).

6. Provisioning and lead times

- 6.1 Delivery follows: discovery and design; account provisioning; onboarding by product family; policy hardening and integration; cut-over and handover. A scoped pilot may be run on the Customer's own traffic before wider rollout. Lead times are indicative only.
- 6.2 The Service Commencement Date for each Protected Asset is the date it is placed in production behind Cloudflare (or, for Zero Trust, the date the first production user group is moved).

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 Cloudflare.
- 7.2 Managed tiers. FirstNet's engineering hours, change allowance and service-review cadence for the managed tier ordered are as stated in the Service Schedule. Any service level for this Service is stated in the Service Schedule; where none is stated, FirstNet uses reasonable endeavours and passes through Cloudflare's service level.
- 7.3 Resilience. FirstNet designs the Service around the Customer's risk tolerance and documents fallback procedures (for example DNS fallback or BGP failover) during onboarding. FirstNet does not quote uptime figures except as stated in the Service Schedule.
- 7.4 Exclusions. FirstNet's own targets do not apply to failures caused by Cloudflare platform incidents, the Customer's Origin, DNS registrar, identity provider or upstream carriers, configuration the Customer approved or changed, attacks beyond the capacity or features of the ordered Cloudflare plan, or force majeure.
- 7.5 FirstNet's own 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. Cloudflare credits passed through under clause 4.6 are not affected.

8. Data, privacy and security

- 8.1 Roles. The Service processes Customer Personal Information, including visitors' and users' IP addresses, request data, identity attributes, logs and (for Gateway, CASB and DLP) the content of traffic. FirstNet processes it as the Customer's operator under POPIA and Cloudflare as FirstNet's sub-operator (or, where the Customer contracts with Cloudflare directly, as the Customer's 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. Access to the Cloudflare Account by FirstNet staff is role-based, uses single sign-on and multi-factor authentication, and is logged.
- 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. Cloudflare processes traffic, configuration, analytics and logs for the Service in the locations Cloudflare publishes for its service; where this is outside South Africa, FirstNet relies on section 72 of POPIA as set out in clause 8.5. Cloudflare offers data localisation options for some products (<https://www.cloudflare.com/data-localization/>); these apply only if named in the Service Schedule.
- 8.5 Cross-border transfers. Any processing outside South Africa described in clause 8.4 is a transfer 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 Cloudflare being bound by its Data Processing Addendum as a binding agreement that provides an adequate level of protection (section 72(1)(a)). Cloudflare's sub-processors are listed at <https://www.cloudflare.com/gdpr/subprocessors/>. The Customer is responsible for informing its data subjects.
- 8.6 Keys. Private keys uploaded by the Customer are stored by Cloudflare under the Vendor Terms and Information Security Exhibit. FirstNet does not keep copies of the Customer's private keys.

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 Charges may depend on the number of Protected Assets, request volumes, users or seats, bandwidth, sites and Prefixes, and add-on modules. Usage above the committed amounts in the Service Schedule (for example request volume, bandwidth or seats) is charged as stated in the Service Schedule.
- 9.3 Cloudflare 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 Onboarding of additional modules, Magic Transit or Magic WAN designs and other project work are quoted separately.

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. Cloudflare Enterprise 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 Cloudflare, the Customer may reduce the quantities (for example Protected Assets, seats or add-on modules) at any time on written notice, down to the minimum quantity Cloudflare sets for the subscription (the "Vendor minimum"). If the Customer cancels during the committed term, the Charges for the Cloudflare 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 Self-serve plans bought monthly may be cancelled on 30 (thirty) days' notice, subject to any minimum period for the FirstNet managed wrap in the Service Schedule.
- 10.4 Exit. Before the Service ends, FirstNet will agree an exit plan with the Customer, which may include: removing the Customer's Cloudflare Account from FirstNet's Cloudflare MSSP organisation and handing full control of it to the Customer, or moving its zones to the Customer's new provider; exporting configuration; moving nameservers or DNS records back to the Customer's chosen provider; withdrawing Prefix advertisements in a coordinated BGP change; and arranging replacement certificates. The Customer must complete its own DNS, registrar and routing changes. Protection stops when the Cloudflare subscription ends.

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 Cloudflare suspends the Service, if the Customer's use creates a security risk or harms others, or if the law or a competent authority requires it.
- 11.2 Because suspension of a proxied domain or Magic Transit may make the Customer's services unreachable, FirstNet will, where reasonably possible, give notice so that the Customer can re-route its traffic.

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 No guarantee against all attacks. The Service reduces the risk and impact of attacks, but no service can stop every attack. Subject to the Agreement, FirstNet is not liable for loss or damage arising from: an attack that exceeds the protection, capacity or features of the ordered Cloudflare plan; a new or unknown attack method; legitimate traffic blocked by rules the Customer approved for enforcement; DNS, registrar, certificate or BGP changes made by the Customer or third parties; compromise of the Customer's Origin, credentials or identity provider; or the Customer's failure to give the notices or obtain the consents in clause 5.8.
- 12.3 Nothing in these SST limits liability that cannot be limited by law.

13. Regulatory notes

- 13.1 ECTA take-down. FirstNet, as an ISPA member, may receive take-down notices under section 77 of the Electronic Communications and Transactions Act 25 of 2002 about content served through the Service. FirstNet may pass the notice to the Customer and act on it as the law allows. Cloudflare handles abuse reports under its own abuse approach.
- 13.2 Traffic inspection. See clause 5.8 (RICA, POPIA and labour law).
- 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 Cloudflare'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 Cloudflare subscription under clause 10.2.
- 14.2 The version number and effective date below identify this version.

Cloudflare Web, DDoS and Zero Trust | 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. Cloudflare Web, DDoS and Zero Trust, v2026.10c. The current version of every FirstNet legal document is at www.firstnet.co.za/legal-notices/.