

SERVICE SPECIFIC TERMS / SECURITY

Managed Firewall

Fortinet and Sophos firewalls, FortiManager and FortiAnalyzer as a Service

VERSION
v2026.10c

EFFECTIVE
1 November 2026

REPLACES
Managed-Firewall-Services.pdf

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/.

Firewall as a Service (Fortinet or Sophos), FortiManager and FortiAnalyzer as a Service

1. Status and precedence

- 1.1 These Service Specific Terms ("SST") apply to every managed firewall Service that FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07) ("FirstNet") provides to the Customer, including Firewall as a Service on Fortinet or Sophos, FortiManager as a managed service and FortiAnalyzer as a 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 What the Customer has ordered (the track, licence bundle, number of firewalls, sites, storage bundle, support hours, MRC, NRC and Initial Period) is set out in the Service Schedule, quote or scope of work signed or 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 **"ADOM"** means an administrative domain in FortiManager or FortiAnalyzer that separates the configuration, policies, objects or logs of one customer, business unit or environment from another.
- 2.2 **"Change Request"** means a request by a Technical Contact to add, change or remove a firewall rule, NAT entry, VPN, route, object, security profile or other configuration item.
- 2.3 **"FAZaaS"** means FortiAnalyzer as a Service: a dedicated FortiAnalyzer virtual machine hosted and operated by FirstNet for the Customer and sold by storage bundle.
- 2.4 **"Firewall"** means the firewall instance used to provide the Service, whether a dedicated appliance at the Customer's site, a virtual domain (VDOM) on FirstNet's hosted FortiGate platform, or a dedicated Sophos Firewall Virtual instance on FirstNet's hosted platform.
- 2.5 **"FirstNet Equipment"** means any Firewall appliance, licence or other equipment that FirstNet supplies to the Customer under the Service and that remains FirstNet's property.
- 2.6 **"Hosted Firewall"** means a Firewall that runs on FirstNet's hosted platform (Fortinet Hosted VDOM Lite or Enterprise, or Sophos Shared Firewall).
- 2.7 **"On-Site Firewall"** means a dedicated Fortinet FortiGate or Sophos XGS appliance installed at the Customer's premises and managed by FirstNet (Fortinet On Prem FWaaS or Sophos On-Premise FWaaS).

- 2.8 **"Security Event"** means an actual or reasonably suspected unauthorised access to, or attack on, the Firewall or the networks it protects.
- 2.9 **"Storage Bundle"** means the FAZaaS storage capacity ordered by the Customer, sold in steps of 50 GB.
- 2.10 **"Technical Contact"** means a person named by the Customer in writing as authorised to log Change Requests and service requests, approve changes and receive security notifications.

3. Service description

- 3.1 Managed firewall tracks. FirstNet provides the Firewall in the track and licence bundle stated in the Service Schedule:
- 3.1.1 Fortinet On Prem FWaaS: a dedicated FortiGate at the Customer's site, managed by FirstNet;
 - 3.1.2 Fortinet Hosted VDOM Lite: a hosted firewall on FirstNet's FortiGate platform for firewalling, NAT, routing, segmentation and site-to-site VPN;
 - 3.1.3 Fortinet Hosted VDOM Enterprise: the Lite features plus the advanced security and networking features stated in the Service Schedule (for example intrusion prevention, antivirus, web filtering, application control, SSL inspection and SD-WAN, where sized for them);
 - 3.1.4 Sophos On-Premise FWaaS: a dedicated Sophos Firewall XGS appliance at the Customer's site, managed through Sophos Central; and
 - 3.1.5 Sophos Shared Firewall: a dedicated Sophos Firewall Virtual instance for the Customer on FirstNet's hosted platform. Each Customer has its own virtual firewall; no firewall instance is shared between customers.
- 3.2 Sophos licence bundles. A Sophos Firewall is licensed with Standard Protection or Xstream Protection, as stated in the Service Schedule. Features available depend on the bundle and on the Vendor's current product.
- 3.3 Management models. The Service is provided in one of these models, as stated in the Service Schedule:
- 3.3.1 Managed: FirstNet alone administers the Firewall, including policy and configuration, through approved Change Requests; or
 - 3.3.2 Delegated administration: the Customer's staff or another provider named by the Customer keeps an agreed administrative role on the Firewall. The Service Schedule records the access each party has. FirstNet is not responsible for the result of changes made by anyone other than FirstNet.
- 3.4 What FirstNet provides in every track:
- 3.4.1 design and baseline configuration of the Firewall from the information the Customer supplies, including zones, segmentation, rules, NAT, routing and VPNs;
 - 3.4.2 for a Fortinet Hosted Firewall, a separate VDOM for the Customer, and for a Sophos Hosted Firewall, a separate virtual machine, so that the Customer's policies and logs are kept apart from other customers';
 - 3.4.3 monitoring of the Firewall's availability and health, and alerts to the Technical Contact on Security Events that FirstNet detects;
 - 3.4.4 firmware, signature and security-update management under a planned firmware programme, applied in agreed maintenance windows except for urgent security fixes;
 - 3.4.5 implementation of approved Change Requests within the change allowance and process in the Service Schedule;
 - 3.4.6 configuration backups and documented rollback for changes; and
 - 3.4.7 the reporting stated in the Service Schedule, which may include monthly summaries of changes, firmware status and licence use.
- 3.5 FortiManager. Where ordered, FirstNet operates FortiManager as the management plane for the Customer's Fortinet devices, with an ADOM designed for the Customer, validated policy packages (install preview before each push), revision history and rollback. FirstNet's default deployment is a FortiManager virtual machine on FirstNet's private cloud in South Africa, in a high-availability pair with daily configuration backups. If FortiManager is unavailable, the Customer's FortiGates keep enforcing their last installed policy.

- 3.6 FortiAnalyzer as a Service (FAZaaS). Where ordered, FirstNet provides a dedicated FortiAnalyzer virtual machine, hosted on FirstNet-operated infrastructure in South Africa, for log collection, analytics and reporting on the Customer's Fortinet devices. FirstNet handles patching, upgrades, backups and capacity monitoring. The following apply:
- 3.6.1 the Storage Bundle is a hard limit. Logs received after the Storage Bundle is full are not stored. FirstNet will alert the Technical Contact before ingestion reaches the limit, and the Customer may order a larger Storage Bundle. FirstNet does not charge for overage, and is not responsible for logs that are not stored because the Customer did not increase the Storage Bundle;
 - 3.6.2 the retention period is a function of the Storage Bundle and the Customer's daily log volume. Retention periods given during sizing are estimates;
 - 3.6.3 FAZaaS is not a security information and event management (SIEM) service. Forwarding logs to the Customer's SIEM is available only if stated in the Service Schedule; and
 - 3.6.4 the Customer must keep the inspection bypasses and minimum firmware versions that FirstNet specifies, so that Fortinet updates and reporting work.
- 3.7 Vendor platform. Fortinet, Inc. provides the FortiGate, FortiManager and FortiAnalyzer software, FortiGuard security updates and FortiCare support. Sophos provides the Sophos Firewall software, Sophos Central, Sophos X-Ops threat intelligence and Sophos support. FirstNet provides the managed service around the Vendor platform and is the Customer's single point of contact.
- 3.8 What is not included. Unless the Service Schedule says otherwise, the Service does not include:
- 3.8.1 the Customer's internal network (LAN, switches, wireless, cabling, servers, workstations, mobile devices), help desk support for end users or applications, or on-site "hands and feet" support;
 - 3.8.2 internet access or other connectivity, which is a separate Service with its own terms;
 - 3.8.3 remote-user internet access, data encryption within the Customer's network, or protocols other than IP;
 - 3.8.4 full network redesigns, security audits, penetration testing, compliance assessments or migration projects, which are scoped separately;
 - 3.8.5 managed detection and response, endpoint protection or incident response on the Customer's systems, which are separate Services (see the Managed Detection and Response Service Specific Terms); and
 - 3.8.6 Fortinet or Sophos hardware or licences sold on their own without a FirstNet managed service, which are supplied under a separate quote and the Vendor Terms only.
- 3.9 Related services. These SST cover firewalls at the Customer's sites and on FirstNet's hosted firewall platform (Fortinet and Sophos). Cloud-delivered web application firewall, DDoS protection, Zero Trust and Magic Firewall services on Cloudflare are covered by the Cloudflare Web, DDoS and Zero Trust Service Specific Terms, and an SD-WAN overlay managed as a separate Service by the Managed SD-WAN and Modern Networking Service Specific Terms.

4. Vendor Terms

- 4.1 The Service uses the following Vendor products, which are subject to the Vendor Terms listed below. The Customer accepts the applicable Vendor Terms when it orders or first uses the Service:
- 4.1.1 Fortinet: Fortinet Product License Agreement / EULA and Warranty Terms (<https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf>), Fortinet Service Terms and Conditions for FortiCare, FortiGuard and other Fortinet service offerings (<https://www.fortinet.com/content/dam/fortinet/assets/legal/Fortinet-Service-Offering-Terms.pdf>), Fortinet Privacy Policy (<https://www.fortinet.com/corporate/about-us/privacy>) and the Fortinet data protection agreement (<https://trust.fortinet.com/product/default/data-protection-addendum>); and
 - 4.1.2 Sophos: Sophos End User Terms of Use (<https://www.sophos.com/en-us/legal/sophos-end-user-terms-of-use>), Sophos Data Processing Addendum (<https://www.sophos.com/en-us/legal/data-processing-addendum>) and Sophos Group Privacy Notice (<https://www.sophos.com/en-us/legal/sophos-group-privacy-notice>).

- 4.2 The Vendor Terms include restrictions on use, such as bans on reverse engineering, modifying or reselling the software and on using it to build a competing product, and export-control restrictions. The Customer must not do anything that would breach those restrictions.
- 4.3 A Vendor may change its products, licence bundles, features, end-of-life dates or Vendor Terms. FirstNet is not liable for those changes. Where a Vendor change materially affects the Service, FirstNet will tell the Customer and the change provisions of the Agreement apply.
- 4.4 A Vendor may suspend or end the Customer's use of its product if the Customer breaches the Vendor Terms. FirstNet is not liable for that suspension.
- 4.5 FirstNet passes through to the Customer the Vendor's warranties for the Vendor product only to the extent FirstNet may do so. FirstNet gives no additional warranty for the Vendor's product. Hardware warranty and replacement (RMA) for an On-Site Firewall are as provided by the Vendor's support contract for that appliance.

5. Customer responsibilities

- 5.1 The Customer must name at least one primary and one back-up Technical Contact before the Service Commencement Date and keep their details current. FirstNet will act on Change Requests, approvals and instructions from Technical Contacts only.
- 5.2 The Customer must give FirstNet complete and accurate information for design and changes, including: users, devices, sites and expected growth; peak inspected throughput and SSL inspection needs; ISP handoff, circuit, public IP and failover details; subnets, VLANs, routing and NAT requirements; VPN peers and remote-user numbers; firewall policy requirements (sources, destinations, ports and published services); certificates; and maintenance windows. FirstNet is not responsible for a fault or security gap caused by incomplete or wrong information.
- 5.3 The Customer must review its architecture with FirstNet, including any change that could weaken the security of the Firewall, FirstNet's network or other customers.
- 5.4 The Customer is responsible for all use of the Service by its systems and users, and for restricting access to its servers by policy, rules and agreements with its contractors and other third parties. Each documented rule must show the Customer addresses, the server addresses and the services (protocols and ports) allowed.
- 5.5 The Customer must use the Service only to reach authorised servers and networks. An attempt to use the Service to access unauthorised servers or networks is a material breach of these SST and of the Acceptable Use Policy.
- 5.6 The Customer must comply with the Acceptable Use Policy, the Vendor Terms and its own information security policies, and must ensure that its staff and contractors do so.
- 5.7 For an On-Site Firewall, the Customer must provide suitable rack space, clean power, environmental conditions and access for installation and replacement, and must keep the appliance in a secure place. FirstNet Equipment at the Customer's premises is at the Customer's risk from delivery until it is returned, and the Customer must insure it against loss and damage. The Service Schedule states whether an On-Site Firewall appliance is FirstNet Equipment or is sold to the Customer; an appliance sold to the Customer becomes the Customer's property as set out in the Service Schedule and the Agreement.
- 5.8 Where the Customer has delegated administration, the Customer must make sure that its staff and providers follow the change process in the Service Schedule and tell FirstNet promptly of any change they make.
- 5.9 The Customer must not ask FirstNet to configure the Service in a way that breaks Applicable Law, including RICA and POPIA (see clause 13).

6. Provisioning and lead times

- 6.1 FirstNet will agree a design and implementation plan with the Customer, including validation, cut-over and rollback steps. Lead times given are indicative only. Lead times for On-Site Firewall appliances depend on Vendor and distributor stock.
- 6.2 The Service Commencement Date is the date FirstNet hands the Service over after validation against the agreed acceptance criteria. If the Customer does not raise a material defect within 5 (five) Business Days after handover, or uses the Service in production, the Service is accepted.

- 6.3 Migration of existing rules from another platform or provider is done on a best-effort basis from the configuration the Customer provides. FirstNet will not be responsible for rules that the Customer did not identify.

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>). Support hours are 8x5 (Business Hours) or 24x7, as stated in the Service Schedule. Priorities and first response times are as set out in that guide.
- 7.2 Availability. Unless the Service Schedule states a different target, FirstNet's availability target for the Service is 99.5% per calendar month, excluding the events in clause 7.5. Availability is measured per calendar month. The target covers Hosted Firewalls, FortiManager and FAZaaS. It does not apply to an On-Site Firewall that is a single hardware appliance without a high-availability pair; FirstNet does not provide Hosted Firewalls on a single appliance. Apart from this target, FirstNet does not guarantee uninterrupted operation.
- 7.2.1 If the availability of the affected Service in a calendar month is below the target, the Customer is entitled to a service credit, calculated as a percentage of the MRC of the affected Service for that calendar month, unless the Service Schedule states a different table:

Availability in the calendar month	Service credit (% of the MRC of the affected Service)
99.5% or more	0%
below 99.5% down to 98%	5%
below 98% down to 97%	10%
below 97% down to 96%	15%
below 96% down to 95%	20%
below 95%	25%

- 7.2.2 For service credits: (a) the Customer must claim in writing within 30 (thirty) days after the end of the calendar month in which the shortfall occurred; (b) only one credit applies per calendar month, being the highest applicable; (c) total credits for a Service in a calendar month may not exceed 25% of the MRC of that Service for that month; and (d) credits are passed as a credit on the next invoice after approval.
- 7.3 Changes. Standard Change Requests are implemented within the time and change allowance stated in the Service Schedule. Emergency changes, after-hours changes and major design changes may need escalation and separate approval and may be charged.
- 7.4 Maintenance. Planned maintenance is done in agreed maintenance windows. FirstNet may do urgent maintenance or apply urgent security fixes at short notice where needed to protect the Service or other customers.
- 7.5 Exclusions. Availability targets and response times do not apply to failures caused by: Vendor platform or cloud outages (including Sophos Central, FortiGuard or FortiCare); planned or emergency maintenance; the Customer's network, power, connectivity or equipment; changes made by the Customer or its delegated administrators; the Customer's failure to follow the change process or to provide information or access; Security Events that the Customer has not remediated; or force majeure.
- 7.6 Service credits under clause 7.2 are the Customer's sole financial remedy for failure to meet the availability target. 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. In providing the Service, FirstNet processes Customer Personal Information (for example IP addresses, user names, device identifiers and the content of logs) as the Customer's operator under POPIA. The Customer is the responsible party. The Data Processing Annexure published at www.firstnet.co.za/legal-notices/ applies.

- 8.2 Confidentiality and instructions. FirstNet will process Customer Personal Information only with the Customer's knowledge or authorisation, for the purpose of providing the Service, and will treat it as confidential.
- 8.3 Security measures. FirstNet will maintain appropriate, reasonable technical and organisational measures to protect Customer Personal Information, as required by section 19 of POPIA, under its information security management system. FirstNet's information security management system is certified to ISO/IEC 27001:2022 by INTERCERT (certificate IC-IS-2512139), with this scope: "The Information Security Management System at FirstNet Technology Services (Pty) Ltd applies to the design, deployment, operation, and support of cloud, connectivity, voice, firewall, and security services, including all associated network infrastructure and technical operations." Management access to the Firewall is limited to authorised FirstNet personnel and, in a delegated model, the people the Customer authorises.
- 8.4 Security compromises. If FirstNet has reasonable grounds to believe that Customer Personal Information it processes for the Service has been accessed or acquired by an unauthorised person, FirstNet will notify the Customer immediately, as required by section 21(2) of POPIA, and give the Customer the information it reasonably needs to assess the compromise. The Customer, as responsible party, decides whether and how to notify the Information Regulator and affected data subjects under section 22 of POPIA. FirstNet will cooperate reasonably.
- 8.5 Where data is held.
- 8.5.1 South Africa by default. FirstNet stores and processes Customer Data for the Service in South Africa, unless the Service Schedule names another site or this clause 8.5 states that a Vendor processes it outside South Africa. Fortinet Hosted Firewalls, FortiManager and FAZaaS run on FirstNet-operated infrastructure in South Africa, and under normal operation the Customer's configuration and logs stay in South Africa.
- 8.5.2 Fortinet devices send device registration, licensing, support and threat-intelligence queries (FortiGuard and FortiCare) to Fortinet, which may process this data outside South Africa. Fortinet processes this data in the locations Fortinet publishes for its service.
- 8.5.3 Sophos Firewalls are managed through Sophos Central, which is hosted outside South Africa in a Sophos region in Ireland or Germany. The region is chosen when the Customer's Sophos Central account is set up, and the Customer may choose which of the two is used. Sophos Central firewall management data, reporting and logs are processed in that region. The Sophos Shared Firewall instance itself runs on FirstNet's platform in South Africa.
- 8.5.4 Where personal information is transferred outside South Africa as described in this clause 8.5, 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 the recipient being bound by the Vendor's data processing addendum as a binding agreement that provides an adequate level of protection (section 72(1)(a)). The Customer, as responsible party, is responsible for informing its data subjects of these transfers.
- 8.6 Logs and data at the end of the Service. The Customer owns its configuration and logs. On request made before the Service ends, FirstNet will export the Firewall configuration and, for FAZaaS, the logs, in the Vendor's standard format. After the Service ends, FirstNet will delete the Customer's configuration and logs once the export period stated in the Service Schedule or agreed exit plan has passed, unless the law requires FirstNet to keep them. Export or migration work beyond the standard export is scoped separately.
- 8.7 No guarantee of security. FirstNet will provide the Service with reasonable skill and care using the security features of the Vendor platform. No firewall or security service can prevent every attack. The Service may not prevent a determined attacker, an attack using a new or unknown method, or an insider with authorised access from gaining access to the Customer's systems or information.

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 The MRC is based on the track, licence bundle, appliance model, Storage Bundle, number of managed devices and support hours in the Service Schedule. Changes to any of them (for example adding a site, moving from Standard to Xstream Protection, adding FortiManager devices or increasing a Storage Bundle) are charged from the next billing cycle.

- 9.3 FortiManager is licensed per managed device. If the number of managed devices exceeds the licensed number, FirstNet will tell the Customer and the Customer must order the additional entitlement.
- 9.4 Vendor 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.
- 9.5 Work outside the scope in the Service Schedule (for example redesigns, migrations, audits, after-hours work the Customer requests, or changes above the change allowance) is charged at FirstNet's then-current rates, after the Customer approves a quote.

10. Term, cancellation and early termination

- 10.1 Each 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 a Service before the end of its Initial Period, the early termination charges in the Agreement apply, unless the Service Schedule states different charges. Where the Customer is a Consumer, FirstNet may charge only a reasonable cancellation penalty as allowed by 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 Where FirstNet has bought a Vendor licence or subscription for a fixed term for the Customer (for example a Fortinet FortiCare or FortiGuard term licence, or an appliance bought for the Customer), and the Service Schedule states that it cannot be cancelled, the cost of that licence or appliance for the rest of its committed term remains payable. Sophos licences that FirstNet buys monthly for the Customer are not committed in this way unless the Service Schedule says so.
- 10.4 At the end of the Service, the Customer must return FirstNet Equipment in good condition (fair wear and tear excepted) within 14 (fourteen) days, or pay its replacement value. FirstNet will decommission Hosted Firewalls and remove the Customer's devices from FortiManager, FAZaaS and Sophos Central after the export in clause 8.6.

11. Suspension

- 11.1 FirstNet may suspend all or part of the Service, on as much notice as is reasonable in the circumstances, if:
- 11.1.1 FirstNet detects, confirms or is notified of unauthorised access, malicious traffic caused by infection, or abuse from the Customer's systems that is harming or is likely to harm FirstNet's network, the Service or other customers;
 - 11.1.2 the Customer breaches the Acceptable Use Policy or the Vendor Terms, or a Vendor suspends the Customer's use;
 - 11.1.3 the Customer does not pay undisputed Charges when due, in accordance with the Agreement; or
 - 11.1.4 suspension is required by law or by a court, regulator or other competent authority.
- 11.2 Where suspension is for a security reason, FirstNet and the Customer will work to resolve the issue. FirstNet will restore the Service as soon as the reason for suspension has been dealt with to FirstNet's reasonable satisfaction. If the issue is not resolved within a reasonable time, FirstNet may terminate the affected Service on notice.
- 11.3 The Customer remains liable for the MRC during a suspension caused by the Customer's breach.

12. Liability specifics

- 12.1 The limitations and exclusions of liability in the Agreement apply to the Service. These SST do not state a separate cap.
- 12.2 Subject to the Agreement, FirstNet is not liable for loss or damage arising from:

- 12.2.1 a Security Event or attack that the Service did not prevent or detect, where FirstNet provided the Service in accordance with these SST;
 - 12.2.2 rules, changes or configuration requested or approved by the Customer, or made by the Customer or its delegated administrators;
 - 12.2.3 logs not stored because the Storage Bundle was full, or not retained because the Customer chose a retention period or Storage Bundle that was too small;
 - 12.2.4 inspection, decryption or blocking that the Customer instructed FirstNet to configure, or the Customer's failure to give the notices or obtain the consents described in clause 13; or
 - 12.2.5 the Customer's failure to remediate a vulnerability or Security Event that FirstNet notified to it.
- 12.3 Nothing in these SST limits liability that cannot be limited by law, including under the CPA where it applies.

13. Regulatory notes

- 13.1 Cybercrimes Act. Under section 54 of the Cybercrimes Act 19 of 2020, an electronic communications service provider that becomes aware that its electronic communications service or network is involved in the commission of certain offences must report this to the South African Police Service within 72 hours and preserve related information. Where this duty applies, FirstNet will comply with it, and the Customer agrees that FirstNet may disclose the information that the law requires.
- 13.2 Traffic inspection (RICA). Features such as SSL/TLS inspection, web filtering and application control examine the content of communications passing through the Firewall. The Customer decides which of these features are enabled and is responsible for ensuring that the inspection is lawful, including under section 6 of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (RICA) (interception in the course of carrying on business, which requires, among other things, that users are informed in advance) and under POPIA. The Customer should exclude categories of sensitive traffic (for example banking and health sites) where appropriate.
- 13.3 Employee monitoring. Where the Customer uses the Service to monitor its employees' internet use, the Customer is responsible for its workplace policies and notices to employees.
- 13.4 Electronic Communications and Transactions Act. FirstNet may act on a lawful take-down notice under section 77 of the Electronic Communications and Transactions Act 25 of 2002 in respect of content hosted on its network.

14. Changes to these terms

- 14.1 FirstNet may update these SST to reflect changes in Vendor products or Vendor Terms, changes in law or regulation, security requirements, or changes in how FirstNet provides the Service. FirstNet will give the Customer 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 without an early termination charge by notice before the change takes effect, except for committed Vendor licences under clause 10.3.
- 14.2 The version number and effective date below identify this version.

Managed Firewall | 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. Managed Firewall, v2026.10c. The current version of every FirstNet legal document is at www.firstnet.co.za/legal-notices/.