

SERVICE SPECIFIC TERMS / SECURITY

Managed Detection and Response

Sophos MDR and managed EDR on Fortinet FortiEDR

VERSION
v2026.10cEFFECTIVE
1 November 2026REPLACES
FortiEDR.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/.

Sophos MDR with FirstNet Incident Response, and managed EDR (including FortiEDR)

1. Status and precedence

- 1.1 These Service Specific Terms ("SST") apply to the managed detection and response and managed endpoint detection and response Services that FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07) ("FirstNet") provides to the Customer, including Sophos Managed Detection and Response (Sophos MDR) with FirstNet Incident Response, related Sophos XDR, NG-SIEM and endpoint products, and managed EDR on Fortinet FortiEDR.
- 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 products, support tier, number of Covered Endpoints and other licensed quantities, telemetry sources, retention, 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 **"Alert"** means a notification of malicious or suspicious activity raised by the Vendor's security operations team or platform.
- 2.2 **"Covered Endpoint"** means a laptop, desktop, server or other device on which the Vendor's agent is installed and licensed under the Service.
- 2.3 **"Incident"** means a confirmed or reasonably suspected compromise of the Customer's systems or data notified to the Customer under the Service.
- 2.4 **"IR Runbook"** means the incident response runbook agreed between FirstNet and the Customer during onboarding, which records how Alerts are received, who is contacted, who may authorise actions, which response mode applies and which remediation playbooks apply.
- 2.5 **"Response Mode"** means the level of authority the Customer gives the Vendor and FirstNet to take response actions without asking first, as recorded in the IR Runbook (see clause 3.4).
- 2.6 **"Telemetry Source"** means a system that sends security data to the Vendor platform, such as endpoints, firewalls, identity, cloud, email or Microsoft Defender.

3. Service description

- 3.1 Two-arm model. The Service has two parts:
 - 3.1.1 Sophos MDR: Sophos provides the 24×7 security operations centre (SOC) layer, which includes threat hunting, analyst-led detection, investigation and Alerts, for Covered Endpoints and integrated Telemetry Sources; and
 - 3.1.2 FirstNet Incident Response: FirstNet's support desk receives Sophos notifications and FirstNet's Incident Response team works with the Customer to contain, remediate and recover, following the IR Runbook.
 - 3.1.3 FirstNet does not operate its own SOC.
- 3.2 FirstNet managed-service wrap. FirstNet provides onboarding, configuration, customer success, compliance reporting and escalation coordination around the Vendor platform, at the support tier stated in the Service Schedule:
 - 3.2.1 Standard: Sophos MDR 24×7 monitoring, threat hunting and analyst-led detection, with FirstNet Incident Response on Sophos notifications, customer success and escalation coordination under the IR Runbook;
 - 3.2.2 Enhanced: Standard plus named FirstNet customer-success engagement, expanded Incident Response support, longer telemetry retention and additional reporting, as stated in the Service Schedule; and
 - 3.2.3 Premium: Enhanced plus extended Incident Response (including on-site remediation support where stated in the Service Schedule), executive reporting and dedicated runbook engineering.
- 3.3 Platform modules. The Service Schedule states which Sophos products are included, which may include Sophos endpoint protection (including Intercept X), XDR, NG-SIEM (telemetry ingestion, log retention and reporting), Secure AI and integrations with Microsoft 365, Azure, AWS, Google Workspace and Microsoft Defender. A module is included only if it is named in the Service Schedule.
- 3.4 Response Modes. The Customer chooses a Response Mode in the IR Runbook. Under Sophos's current service description:
 - 3.4.1 Authorise: Sophos may take response actions (for example isolating a device or killing a process) without asking first, and notifies afterwards;
 - 3.4.2 Collaborate: Sophos asks for consent before most response actions; and
 - 3.4.3 Notify only: Sophos investigates and gives guidance, and the Customer (with FirstNet where in scope) takes the actions.
 - 3.4.4 The Customer acknowledges that choosing Collaborate or Notify only may delay containment, and that the Customer bears the consequences of a delay caused by its choice or by its failure to respond to a request for consent.
- 3.5 Managed EDR on FortiEDR. Where the Service Schedule includes FortiEDR, FirstNet provides Fortinet's cloud-based endpoint protection platform for the Covered Endpoints and, where ordered, alert management in which FirstNet reviews events in the FortiEDR console, acts on them and contacts the Customer about malicious events. Alert-handling targets are: malicious and suspicious events within 24 (twenty-four) hours, and inconclusive, potentially unwanted and safe events within 48 (forty-eight) hours, of the event being generated in the console. These are targets, not guarantees, and are measured from the event being generated in the console (not from the start point in clause 7.2). Sophos is FirstNet's main endpoint platform; FortiEDR is available on request. This clause 3.5 and the other FortiEDR terms in these SST apply wherever the Service Schedule includes FortiEDR. FortiEDR licences must be bought through FirstNet.
- 3.6 Onboarding. Onboarding covers discovery and architecture review, a deployment plan, validation of Telemetry Sources, Sophos MDR onboarding and the IR Runbook, and handover to the FirstNet managed-services team.
- 3.7 Incident response scope and limits. FirstNet's Incident Response is limited to the Customer's environment covered by the Service, delivered remotely and in English unless the Service Schedule says otherwise, and to the time allowance (if any) in the Service Schedule. It does not include, unless separately agreed in writing:
 - 3.7.1 rebuilding or re-imaging endpoints or servers, reinstalling operating systems or applications, or restoring data from backup;

- 3.7.2 decryption of encrypted data, ransomware negotiation or payment, or dealing with threat actors;
 - 3.7.3 forensic investigation to evidential standard, expert witness services, or preparing reports for court or regulators;
 - 3.7.4 legal, regulatory or insurance advice, including advice on whether to notify the Information Regulator, data subjects, the police, insurers or other regulators;
 - 3.7.5 public relations or crisis communications; or
 - 3.7.6 incidents that started before the Service Commencement Date, or that affect systems that are not Covered Endpoints or integrated Telemetry Sources.
 - 3.7.7 Work outside this scope is provided only at FirstNet's discretion and is charged at FirstNet's then-current rates.
- 3.8 What is not included. The Service does not include escalation to the Vendor for advanced analysis beyond what the Vendor provides under its service, firewall management (see the Managed Firewall Service Specific Terms), email security, backup (which may be ordered separately, for example Druva backup), or penetration testing.

4. Vendor Terms

- 4.1 The Service uses Vendor products subject to the following Vendor Terms, which the Customer accepts when it orders or first uses the Service:
- 4.1.1 Sophos: Sophos End User Terms of Use (<https://www.sophos.com/en-us/legal/sophos-end-user-terms-of-use>); Sophos Managed Detection and Response Service Description (<https://www.sophos.com/en-us/legal/mdr-description>); Sophos Data Processing Addendum (<https://www.sophos.com/en-us/legal/data-processing-addendum>); Sophos Group Privacy Notice (<https://www.sophos.com/en-us/legal/sophos-group-privacy-notice>); and
 - 4.1.2 Fortinet (FortiEDR): Fortinet Product License Agreement / EULA and Warranty Terms (<https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf>); Fortinet Service Terms and Conditions (<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>).
- 4.2 Under the Sophos MDR service description, where a Customer buys through a partner, the partner acts as the Customer's contact with Sophos and must obtain the Customer's consents for Sophos's response actions. The Customer authorises FirstNet to give those consents on its behalf in accordance with the IR Runbook and Response Mode, and to receive Sophos notifications.
- 4.3 The Vendor Terms restrict use, including bans on reverse engineering, resale and use to build competing products, and Sophos's right to suspend use if there is a significant threat or a breach. The Customer must not breach those restrictions. The Service is for the Customer's internal business use only and may not be resold or used to provide managed services to others unless FirstNet agrees in writing.
- 4.4 Vendors may change their products, service descriptions 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 FirstNet passes through Vendor warranties and service levels only to the extent it is allowed to, and does not add its own. Any Vendor breach-protection warranty applies only if the Service Schedule expressly includes it.

5. Customer responsibilities

- 5.1 Minimum requirements. The Customer must meet the minimum system requirements that FirstNet and the Vendor specify for the agent and Telemetry Sources, as updated from time to time and given to the Customer on request. FirstNet is not obliged to provide the Service for endpoints that do not meet them.
- 5.2 Deployment. The Customer must deploy the agent to the Covered Endpoints and keep it running and up to date. Sophos's service description requires deployment to at least 80% of the licensed quantity for its service to apply. The number of Covered Endpoints may not exceed the number in the Service Schedule.

- 5.3 Contacts and availability. The Customer must name at least one primary and one alternate authorised contact, keep their details current, monitor email and phone messages from FirstNet and the Vendor, and acknowledge priority Alerts promptly (Sophos asks for acknowledgement within 60 minutes where commercially reasonable).
- 5.4 IR Runbook. The Customer must agree the IR Runbook during onboarding, choose a Response Mode, and keep the IR Runbook current when its people, systems or risk appetite change.
- 5.5 Remediation. The Customer must remediate vulnerabilities and compromises that FirstNet or the Vendor reports within 14 (fourteen) days of notification, or sooner if FirstNet advises that the risk is critical. Response targets do not apply to systems awaiting remediation more than 14 days after notification.
- 5.6 Information and cooperation. The Customer must give FirstNet timely information, access, approvals and resources needed to deliver the Service, including relevant application knowledge and data needed to reproduce the conditions in which an Alert occurred, and must assign qualified staff to work with FirstNet.
- 5.7 Connectivity. The Service depends on an adequate and stable internet connection from the Covered Endpoints and Telemetry Sources to the Vendor's cloud.
- 5.8 Policies and lawful use. The Service supplements, but does not replace, the Customer's own security and acceptable-use policies. The Customer must use the Service only for lawful internal cybersecurity purposes, and must check that its use complies with the laws that apply to it before deployment, including the notices and consents described in clauses 8 and 13.
- 5.9 Backups. The Customer is responsible for maintaining independent backups of its systems and data.
- 5.10 Indemnity. The Customer indemnifies FirstNet against claims, losses, penalties and reasonable legal costs arising from the Customer's breach of these SST, the Vendor Terms or the law in using the Service, or from the Customer's failure to obtain the notices and consents for which it is responsible.

6. Provisioning and lead times

- 6.1 Lead times are indicative. Standard MDR onboarding typically takes two to four weeks; XDR or NG-SIEM integration typically takes four to eight weeks depending on the number of Telemetry Sources; replacing a legacy SIEM typically takes eight to sixteen weeks.
- 6.2 The Service Commencement Date for each component is the date FirstNet confirms that the Covered Endpoints are reporting to the Vendor platform and the IR Runbook has been handed over, or the date the Customer starts relying on the Service, if earlier.

7. Service levels and support

- 7.1 Support. Service requests are logged 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>). Priorities and first response times are as set out in that guide. A Sophos Alert that indicates an active Incident is handled as Priority 1.
- 7.2 Service levels. FirstNet Incident Response mobilisation times and any availability targets are those stated in the Service Schedule; where none is stated, FirstNet uses reasonable endeavours and passes through the Vendor's service level. All targets are reasonable-efforts targets measured from receipt of the Alert in FirstNet's support desk or the Vendor console, except the FortiEDR alert-handling targets in clause 3.5, which are measured as stated there.
- 7.3 Exclusions. Targets do not apply to delays or failures caused by: scheduled or emergency maintenance of the Vendor platform; Vendor platform or cloud outages; changes made by the Customer or by others on its behalf; the Customer's failure to follow FirstNet's processes, to respond to requests for consent, or to keep contact details current; acts or omissions of the Customer, its staff, contractors or vendors; breach of these SST; events outside FirstNet's reasonable control; components FirstNet is not responsible for (including the Customer's power, network, hardware, software and content); or systems FirstNet cannot reasonably reach.
- 7.4 Maintenance. Vendors carry out scheduled maintenance of their cloud platforms. During maintenance the console may be briefly unavailable; endpoint protection continues to operate locally. FirstNet may carry out emergency maintenance at short notice if the integrity of the Service is at risk.

- 7.5 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 names, device names, IP addresses, process and file information, email addresses, and security telemetry that may contain the content of files or communications. FirstNet processes it as the Customer's operator under POPIA and the Vendor processes it 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, and will treat it as confidential. FirstNet will maintain appropriate, reasonable technical and organisational measures as required by section 19 of POPIA.
- 8.3 Security compromises affecting FirstNet. If FirstNet has reasonable grounds to believe that Customer Personal Information it or the Vendor 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.
- 8.4 Incidents in the Customer's environment. Where the Service detects an Incident in the Customer's own systems, the Customer, as responsible party, decides whether and how to notify the Information Regulator, data subjects, the police, insurers or other regulators. FirstNet will provide the Incident information it holds to help the Customer do so.
- 8.5 Where data is held. FirstNet's own records for the Service (tickets, IR Runbook and reports) are held in South Africa by default. The Vendor platforms are cloud services:
- 8.5.1 Sophos Central and Sophos MDR are 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. Customer Personal Information processed in them is processed in that region and by the Sophos operations teams that support the service. Sophos's sub-processor list is published at <https://www.sophos.com/en-us/legal/sub-processor>; and
- 8.5.2 Where the Service Schedule includes FortiEDR, the FortiEDR cloud platform is hosted in Fortinet's European Union (EU) region, and FortiEDR data is processed there.
- 8.6 Cross-border transfers. The Sophos platforms (Ireland or Germany) and the FortiEDR platform (EU) involve transferring Customer Personal Information outside South Africa. 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 Vendor being bound by its data processing addendum as a binding agreement that provides an adequate level of protection (section 72(1)(a)). The Customer is responsible for informing its data subjects (including employees) of the transfer and, where it relies on consent, for obtaining it.
- 8.7 Vendor use of security data. Under the Vendor Terms, Vendors may use security and threat-intelligence data derived from the Service to improve their products and for threat research. New information that the Service gives the Customer (for example that a file or address is malicious) may be used by the Customer only for its lawful internal cybersecurity purposes.
- 8.8 Customer's warranty. The Customer warrants that it has the rights, notices and consents needed to give FirstNet and the Vendor the personal information processed by the Service, and to let them process it to provide the Service, prevent and address technical problems and breaches of the Service, and as required by law.
- 8.9 Retention and exit. Telemetry is retained for the period that applies to the products and tier in the Service Schedule. On request made before the Service ends, FirstNet will provide the Customer's Incident reports and, where the Vendor platform allows, an export of the Customer's data. After the Service ends, the Customer's instance and data are kept only for the period stated in the Service Schedule or, if none is stated, for the period the Vendor platform allows, and are then deleted, subject to the Vendor Terms and the law.

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 are based on the number of Covered Endpoints, users, Telemetry Sources, data volumes or retention tiers and the support tier. If actual usage exceeds the licensed quantity, FirstNet may invoice the excess from the month in which it occurred.
- 9.3 The Service is available only to Customers who buy the Vendor licences through FirstNet.
- 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 Incident Response work beyond the allowance in the Service Schedule, and work excluded by clause 3.7, is charged at FirstNet's then-current rates.

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. 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 Where FirstNet has bought a Vendor licence for a fixed term for the Customer and the Service Schedule states that it cannot be cancelled, the Charges for that licence for the rest of its committed term remain payable.
- 10.4 At the end of the Service the Customer must uninstall, or allow FirstNet to uninstall, the Vendor agents. Endpoints stop being protected when licences end.

11. Suspension

- 11.1 FirstNet may permanently or temporarily limit or suspend the Service, on as much notice as is reasonable in the circumstances, if continuing to provide it may compromise the integrity or security of the Service or of FirstNet's or the Vendor's systems, if the Customer does not pay undisputed Charges when due, if the Customer breaches the Acceptable Use Policy or the Vendor Terms, if a Vendor suspends the Service, or if the law or a competent authority requires it.

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 The Service is subject to inherent technical limits. It helps to prevent, detect and contain malware and security breaches, but no security product or service can detect or stop all threats. Subject to the Agreement, FirstNet is not liable for loss or damage arising from:
 - 12.2.1 a failure of the Vendor platform to detect malware or malicious activity, or from false positives, where FirstNet provided the Service in accordance with these SST;
 - 12.2.2 response actions taken in accordance with the Response Mode and IR Runbook, or delays caused by the Customer's choice of Response Mode or failure to respond;
 - 12.2.3 the Customer's failure to remediate within the period in clause 5.5;
 - 12.2.4 data loss or corruption, or the need to rebuild endpoints, where the Customer did not keep adequate backups; or
 - 12.2.5 the Customer's failure to give notices or obtain consents for which it is responsible.

12.3 Nothing in these SST limits liability that cannot be limited by law.

13. Regulatory notes

- 13.1 Cybercrimes Act. Section 54 of the Cybercrimes Act 19 of 2020 requires an electronic communications service provider or financial institution that becomes aware that its electronic communications service or network is involved in the commission of certain cybercrimes to report the offence to the South African Police Service within 72 hours and to preserve related information. Where this duty applies to FirstNet, FirstNet will comply with it and may disclose the information that the law requires. Where the Customer is itself a financial institution or electronic communications service provider, the Customer is responsible for its own reporting duty. The Service does not report Incidents to the police on the Customer's behalf.
- 13.2 Monitoring of users (RICA and POPIA). The Service monitors the activity of the Customer's users on Covered Endpoints and connected systems, and may collect the content of communications or files. The Customer is responsible for ensuring that this monitoring is lawful, including by informing its users in advance as required by section 6 of RICA, and by having a lawful basis and giving notice under POPIA.
- 13.3 Evidence. Information collected by the Service may be needed as evidence. The Customer should tell FirstNet promptly if it intends to involve the police or take legal action, so that information can be preserved.

14. Changes to these terms

- 14.1 FirstNet may update these SST to reflect changes in Vendor products, service descriptions 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 committed Vendor licences under clause 10.3.

- 14.2 The version number and effective date below identify this version.

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