

## SERVICE SPECIFIC TERMS / SECURITY

# Email Security: DMARC and Sophos Email

Managed DMARC powered by Sendmarc, and Sophos Email

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/](http://www.firstnet.co.za/legal-notices/).

Service Specific Terms for managed DMARC (Sendmarc) and Sophos Email, delivered by FirstNet

## 1. Status and precedence

- 1.1 These Service Specific Terms ("SST") apply to the following Services that FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07) ("FirstNet") provides to the Customer: managed DMARC on the Sendmarc platform ("Managed DMARC"), including optional BIMi and brand-impersonation takedown add-ons; and Sophos Email.
- 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/](http://www.firstnet.co.za/legal-notices/).
- 1.3 The in-scope domains, add-ons, number of mailboxes, 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 **"BIMI"** means Brand Indicators for Message Identification, a DNS standard that lets supporting mailbox providers display a verified brand logo next to authenticated email.
- 2.2 **"DMARC"**, **"SPF"** and **"DKIM"** mean the email authentication standards Domain-based Message Authentication, Reporting and Conformance, Sender Policy Framework and DomainKeys Identified Mail.
- 2.3 **"DMARC Policy"** means the policy published in a domain's DMARC record: p=none (monitor only), p=quarantine or p=reject.
- 2.4 **"DMARC Reports"** means the aggregate (RUA) and, where mailbox providers send them, forensic (RUF) reports that receiving mail servers send about email using the Customer's domains.
- 2.5 **"In-Scope Domain"** means each domain listed in the Service Schedule.
- 2.6 **"Sending Source"** means any system or third-party platform that sends email using an In-Scope Domain, such as Microsoft 365, Google Workspace, marketing, CRM, ERP, finance or bespoke applications.
- 2.7 **"VMC"** means a Verified Mark Certificate, a certificate backed by a registered trade mark that most mailbox providers require before displaying a BIMi logo.

### 3. Service description

- 3.1 Managed DMARC: what FirstNet provides. FirstNet runs a managed journey for each In-Scope Domain:
- 3.1.1 discovery of the Customer's domains and Sending Sources;
  - 3.1.2 publication (by the Customer, or by FirstNet with the Customer's authority) of a monitoring-only DMARC record, or use of the Customer's existing record, and collection of DMARC Reports on the Sendmarc platform;
  - 3.1.3 classification of each Sending Source as legitimate, forwarder or unauthorised, shared with the Customer;
  - 3.1.4 specification of the SPF and DKIM changes needed to authenticate each legitimate Sending Source, and validation after the Customer makes them;
  - 3.1.5 a phased move of the DMARC Policy from p=none to p=quarantine to p=reject, with a go or no-go review agreed with the Customer before each step and a rollback path; and
  - 3.1.6 after enforcement, a monthly managed-service review covering enforcement status, new Sending Sources, threat patterns and recommended actions.
- 3.2 Managed DMARC add-ons. If named in the Service Schedule:
- 3.2.1 BIMI: FirstNet configures the BIMI record, arranges hosting of the logo file and assists the Customer to obtain a VMC. BIMI is available only once the DMARC Policy is p=quarantine or p=reject, and only supporting mailbox providers display the logo; and
  - 3.2.2 brand-impersonation takedown: detection of look-alike domains and phishing infrastructure and a takedown request workflow. Takedown depends on the cooperation of registrars, hosts and other third parties and is not guaranteed.
- 3.3 Sophos Email. Where named in the Service Schedule, FirstNet provides Sophos Email, a cloud email security gateway managed through Sophos Central that filters inbound (and, where configured, outbound) email for spam, malware, phishing and impersonation for the licensed mailboxes. FirstNet configures the policies, directory integration and mail routing, and supports and tunes the service. Sophos Email may also be provided as Sophos Firewall Email Protection where the Service Schedule says so.
- 3.4 What the Vendors provide. Sendmarc provides the DMARC platform, DMARC Report processing and hosted records. Sophos provides the Sophos Email platform and Sophos Central.
- 3.5 What is not included. Unless the Service Schedule says otherwise, the Service does not include: changes to the Customer's DNS or Sending Sources (which the Customer makes; see clause 5); administration of the Customer's mail platform; the cost of a VMC or trade mark registration; protection against look-alike or typo-squat domains (DMARC protects only the Customer's own domains); inbound protection for Managed DMARC (which is outbound brand protection only); and any guarantee of compliance with POPIA, an insurer's requirements or an audit.
- 3.6 Related services. These SST cover Managed DMARC on the Sendmarc platform and Sophos Email only. Mimecast email security, including any DMARC module bought as part of a Mimecast package, is covered by the Email Security: Mimecast Service Specific Terms.

### 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 Sendmarc: Sendmarc Terms of Service (<https://sendmarc.com/terms-of-service/>, last updated 5 October 2026), including Appendix 1 (Channel Partners), and the Sendmarc Data Processing Addendum (<https://sendmarc.com/dpa/>); 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 Sendmarc Terms of Service apply to end customers who use the Sendmarc services through a channel partner. FirstNet may not change them or make promises on Sendmarc's behalf.
- 4.3 Vendors may change their products 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 A Vendor may suspend the Service for actual or threatened breach of its terms, suspected unauthorised activity or non-payment. FirstNet is not liable for that suspension.
- 4.5 The Vendors provide their services "as is" and "as available" except as stated in the Vendor Terms. FirstNet passes through Vendor warranties only to the extent it is allowed to and does not add its own.

## 5. Customer responsibilities

- 5.1 DNS authority. The Customer owns and controls its domains and DNS, and is the only party with authority to change them. The Customer must make, or give FirstNet written authority to make, each DNS change needed for the Service (including DMARC, SPF, DKIM, BIMI and MX records, and any delegation of records to Sendmarc). Each DNS change and each DMARC Policy step requires the prior approval of a Technical Contact.
- 5.2 Delegated records. Where the Customer delegates its DMARC (or other) records to Sendmarc so that they can be managed on the Sendmarc platform, the Customer authorises Sendmarc and FirstNet to manage those records within the scope of the Service. The Customer may revoke the delegation at any time by notice, which may end the Service for that domain.
- 5.3 Sending Sources. The Customer must identify the business owner of each Sending Source and make the authentication changes FirstNet specifies on its own platforms and with its third-party providers within the agreed time. The pace of enforcement depends on these changes. FirstNet does not commit to a date for reaching p=reject.
- 5.4 Accuracy. The Customer must confirm which Sending Sources are legitimate. FirstNet relies on that confirmation when recommending enforcement.
- 5.5 Technical Contacts. The Customer must name at least one primary and one back-up Technical Contact and keep their details current.
- 5.6 BIMI and VMC. The Customer is responsible for its trade mark registration and for meeting the certificate authority's requirements for a VMC, and for the logo it supplies.
- 5.7 Sophos Email. The Customer must configure its mail platform as FirstNet specifies (including MX records and connectors), keep the licensed mailbox count accurate, and comply with the Vendor Terms.
- 5.8 The Customer must comply with the Acceptable Use Policy.

## 6. Provisioning and lead times

- 6.1 The first DMARC Reports typically arrive within two reporting cycles after the monitoring record is published. The time to reach p=reject depends mainly on the number of Sending Sources and how quickly the Customer completes authentication changes, and is not committed in advance.
- 6.2 Lead times are indicative only. The Service Commencement Date for Managed DMARC is the date the first In-Scope Domain begins reporting to the Sendmarc platform; for Sophos Email it is the date mail for the first domain flows through Sophos Email in production.

## 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/](http://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 the Vendor; the Customer does not deal with the Vendor directly.
- 7.2 Service levels. Any service level for this Service is stated in the Service Schedule; where none is stated, FirstNet uses reasonable endeavours and passes through the Vendor's service level. The Vendor platforms are provided under the Vendor Terms.

- 7.3 Exclusions. Targets do not apply to failures caused by Vendor platform outages, the Customer's DNS provider, DNS propagation delays, changes made by the Customer or its providers, receiving mailbox providers' behaviour, the Customer's failure to make or approve changes, 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. DMARC Reports contain IP addresses, sending domains and, in forensic reports, parts of messages that may include email addresses and other personal information. Sophos Email processes the content of email. FirstNet processes Customer Personal Information as the Customer's operator under POPIA and the Vendors as FirstNet's sub-operators. The Customer is the responsible party. The Data Processing Annexure published at [www.firstnet.co.za/legal-notices/](http://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.
- 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. The Vendor platforms are hosted as follows:
- 8.4.1 Sendmarc processes Managed DMARC data in the locations Sendmarc publishes for its service; where this is outside South Africa, FirstNet relies on section 72 of POPIA as set out in clause 8.5; and
  - 8.4.2 Sophos Email and Sophos Central 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, including the content of email, is processed in that region.
- 8.5 Cross-border transfers. The transfers outside South Africa described in clause 8.4 are 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 each Vendor being bound by its data processing terms, which FirstNet relies on to provide an adequate level of protection (section 72(1)(a)). The Customer is responsible for informing its data subjects.
- 8.6 Exit. On cancellation, the Customer has 90 (ninety) days to export its Managed DMARC data before it is deleted, in line with the Sendmarc channel partner terms. Before the Service ends, the Customer must take back control of any DNS records delegated to Sendmarc and publish its own DMARC, SPF and BIMI records. If the Customer does not, mail authentication for its domains may fail when the delegated records are removed.

## 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 Managed DMARC is charged per In-Scope Domain, plus any add-ons. Domains discovered during the Service are added only with the Customer's approval and are charged from the next billing cycle. Sophos Email is charged per mailbox.
- 9.3 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.

## 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 subscription for a fixed term for the Customer and the Service Schedule states that it cannot be cancelled, the Charges for that subscription for the rest of its committed term remain payable.

## 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 a Vendor suspends the Service, if the Customer's use creates a security risk, or if the law or a competent authority requires it.
- 11.2 Before suspending Managed DMARC for non-payment, FirstNet will give the Customer reasonable notice so that it can take back control of delegated DNS records.

## 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 Deliverability. Moving a domain to p=quarantine or p=reject causes receiving mail servers to quarantine or reject email that fails authentication. FirstNet recommends each step only after review, but cannot guarantee that every legitimate Sending Source has been found. Subject to the Agreement, FirstNet is not liable for email that is not delivered, is delivered to spam folders or is rejected because of: a DMARC Policy step the Customer approved; a Sending Source the Customer did not disclose or did not authenticate; a DNS change made by the Customer or its DNS provider; or the decisions of receiving mailbox providers, which FirstNet does not control.
- 12.3 No guarantee against spoofing. DMARC at p=reject helps prevent others from sending email that uses the Customer's exact domain, where the receiving server enforces DMARC. It does not stop look-alike domains, compromised accounts at legitimate senders, or receivers that do not enforce DMARC. Sophos Email does not block all malicious email or deliver all legitimate email.
- 12.4 BIML. FirstNet does not guarantee that a VMC will be issued or that any mailbox provider will display the Customer's logo.
- 12.5 Nothing in these SST limits liability that cannot be limited by law.

## 13. Regulatory notes

- 13.1 Email inspection. Sophos Email scans the content of email. The Customer is responsible for informing its users, in its policies, that their email is scanned and filtered, as required for interception in the course of business under section 6 of RICA and for processing under POPIA.
- 13.2 DNS and domain names. The Customer remains the registrant of its domains. Domain registration, ZA domain rules and registrar terms are outside this Service unless FirstNet provides domain services under separate terms.
- 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 Vendor products 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/](http://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 subscriptions under clause 10.3.

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

Email Security: DMARC and Sophos Email | 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](mailto:support@firstnet.co.za)

---

Published by FirstNet Technology Services (Pty) Ltd, registration number 2006/031608/07. Email Security: DMARC and Sophos Email, v2026.10c. The current version of every FirstNet legal document is at [www.firstnet.co.za/legal-notices/](http://www.firstnet.co.za/legal-notices/).