

SERVICE SPECIFIC TERMS / SECURITY

Microsoft 365 Security and Compliance

Assessment, hardening and monitoring of Microsoft 365

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 Microsoft 365 security and compliance Services that FirstNet Technology Services (Pty) Ltd (registration number 2006/031608/07) ("FirstNet") provides to the Customer, whether as a once-off assessment or hardening project, or as an ongoing managed service.
- 1.2 These SST form part of the agreement between FirstNet and the Customer, which is either the FirstNet Standard Terms and Conditions or the Customer's signed Master Services Agreement with FirstNet (the "Agreement"). They are incorporated into the Agreement by reference and are published at www.firstnet.co.za/legal-notices/.
- 1.3 The scope (assessment, implementation, monitoring and enablement activities), the Microsoft workloads and controls in scope, deliverables, MRC, NRC and Initial Period are set out in the Service Schedule, statement of work or quote accepted by the Customer (the "Service Schedule").
- 1.4 Microsoft licences are not supplied under these SST. Where FirstNet supplies them, the Microsoft Cloud (CSP) Service Specific Terms apply to them.
- 1.5 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 Microsoft's products may be used, the Customer must comply with that restriction.
- 1.6 Words defined in the Agreement have the same meaning in these SST.

2. Definitions

- 2.1 **"Admin Access"** means the administrative roles in the Tenant that the Customer grants to FirstNet, including through Microsoft's granular delegated admin privileges (GDAP).
- 2.2 **"Baseline"** means the set of security and compliance policies agreed with the Customer for the Tenant, such as multi-factor authentication, conditional access, device compliance, data loss prevention, sensitivity labels and retention policies.
- 2.3 **"Break-Glass Account"** means an emergency access account in the Tenant that is excluded from conditional access policies so that the Customer can regain access if policies lock administrators out.
- 2.4 **"Tenant"** means the Customer's Microsoft 365 and Microsoft Entra ID tenant.
- 2.5 **"Technical Contact"** means a person named by the Customer in writing, or in the Service Schedule, as authorised to log requests, approve the Baseline and policy changes, and receive security notifications for the Service.

3. Service description

- 3.1 **Assessment.** Where in scope, FirstNet reviews the Tenant's configuration (for example Microsoft Secure Score, identity and access, device management, email and collaboration security, data protection and audit settings), identifies gaps against the Customer's risk profile and compliance needs, and delivers a prioritised action plan.

- 3.2 Implementation. Where in scope, FirstNet designs and implements the agreed Baseline using staged rollouts and change control, which may cover:
- 3.2.1 identity security: multi-factor authentication, conditional access, privileged identity management and identity protection in Microsoft Entra ID;
 - 3.2.2 device and application control: device compliance and configuration through Microsoft Intune, and application governance;
 - 3.2.3 threat protection: Microsoft Defender for Office 365 (safe links, safe attachments, anti-phishing) and other Defender workloads;
 - 3.2.4 data protection: Microsoft Purview data loss prevention, sensitivity labels, encryption and retention; and
 - 3.2.5 compliance: audit logging, eDiscovery and compliance reporting.
- 3.3 Monitoring. Where in scope, FirstNet provides dashboards and reviews of security incidents, configuration drift and user risk signals at the cadence in the Service Schedule, and forwards alerts and logs to the Customer's SIEM where stated. Monitoring is not a 24x7 security operations centre unless the Service Schedule includes the Managed Detection and Response Service.
- 3.4 Enablement. Where in scope, FirstNet provides administrator and end-user training to sustain the Baseline.
- 3.5 Related services. CASB and DLP across other SaaS and AI tools may be provided through Netskope or Cloudflare, and DMARC through Sendmarc, under their own Service Specific Terms. Microsoft 365 backup is a separate Service. Microsoft licences that FirstNet supplies are covered by the Microsoft Cloud (CSP) Service Specific Terms; these SST cover only the security and compliance services described in this clause 3.
- 3.6 What is not included. Unless the Service Schedule says otherwise, the Service does not include: Microsoft licences (see clause 1.4); day-to-day user administration or help desk support; incident response or forensic investigation; migration of data or mailboxes; legal advice on retention periods, legal holds or privacy; or any guarantee of compliance with POPIA, ISO standards, insurer requirements or other frameworks.

4. Vendor Terms

- 4.1 The Customer's use of Microsoft products is governed by the Microsoft Customer Agreement (<https://www.microsoft.com/licensing/docs/customeragreement>), Microsoft's Product Terms (<https://www.microsoft.com/licensing/terms/>) and the Microsoft Products and Services Data Protection Addendum (<https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA>), as described in the Microsoft Cloud (CSP) Service Specific Terms. Those terms are between the Customer and Microsoft.
- 4.2 FirstNet configures only features that the Customer is licensed for. Some controls require specific licences (for example Microsoft Entra ID P1 or P2, Defender for Office 365 Plan 2, or Microsoft 365 E5 compliance features). FirstNet will tell the Customer where a recommended control needs a licence the Customer does not have.
- 4.3 Microsoft may change its products, features, licence requirements, default settings and Vendor Terms. FirstNet is not liable for those changes, including Microsoft changes that alter how a configured policy behaves. Where a change materially affects the Service, FirstNet will tell the Customer and the change provisions of the Agreement apply.
- 4.4 FirstNet gives no warranty for Microsoft's products and passes through Microsoft's warranties and service levels only as described in the Microsoft Cloud (CSP) Service Specific Terms.

5. Customer responsibilities

- 5.1 Admin Access. The Customer must grant FirstNet the Admin Access stated in the Service Schedule, using least-privilege GDAP roles for a defined period. The Customer may review and revoke Admin Access at any time, and must tell FirstNet if it does, since this may stop the Service.
- 5.2 Break-Glass Accounts. The Customer must keep at least two Break-Glass Accounts with strong credentials stored securely by the Customer, excluded from conditional access as FirstNet recommends, and monitored.

- 5.3 Approval of changes. The Customer must approve the Baseline and each material policy change through a Technical Contact before FirstNet applies it to production. The Customer is responsible for communicating changes to its users.
- 5.4 Legal decisions. The Customer decides, and is responsible for, retention periods, legal holds, eDiscovery searches, data classification, DLP rules and the monitoring of users. FirstNet configures these on the Customer's instructions.
- 5.5 Information and cooperation. The Customer must give FirstNet accurate information about its users, devices, applications, third-party integrations and compliance obligations, and make its staff available.
- 5.6 Licences. The Customer must hold the Microsoft licences needed for the controls in scope.
- 5.7 The Customer must comply with the Acceptable Use Policy and the Vendor Terms.

6. Provisioning and lead times

- 6.1 Projects are delivered in the phases in the Service Schedule (typically assessment, Baseline design, staged rollout to a pilot group, then production). Timelines are indicative only and depend on the Customer's approvals and readiness.
- 6.2 Project deliverables are accepted when the Customer signs them off, or 5 (five) Business Days after delivery if the Customer has not raised a material non-conformity. The Service Commencement Date of an ongoing managed service is the date stated in the Service Schedule or, if none, the date the Baseline is applied to 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/ (currently <https://www.firstnet.co.za/api/media/file/SOP-SVC-RR-001-Rapid-Response-Services-Guide.pdf>). A lock-out of administrators or a large group of users caused by a policy change is handled as Priority 1.
- 7.2 Service levels. Response, change and reporting commitments for any managed service are stated in the Service Schedule; where none is stated, FirstNet uses reasonable endeavours. Microsoft's service levels for its products apply as described in the Microsoft Cloud (CSP) Service Specific Terms.
- 7.3 Exclusions. Commitments do not apply to failures caused by Microsoft service incidents, Microsoft changes, changes made by the Customer or other providers in the Tenant, missing licences, revoked Admin Access, 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. In providing the Service, FirstNet accesses the Tenant and may view Customer Personal Information (for example user identities, sign-in logs, device information, audit logs, and where needed for troubleshooting, email or file metadata). FirstNet does this 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. Microsoft processes Tenant data under its contract with the Customer, not as FirstNet's sub-operator.
- 8.2 FirstNet will access and process Customer Personal Information only as needed to provide the Service or as the Customer instructs, will treat it as confidential, and will maintain appropriate, reasonable security measures as required by section 19 of POPIA, including multi-factor authentication and named accounts for all FirstNet staff with Admin Access. FirstNet will not open the content of email or files except where needed for a task the Customer has requested.
- 8.3 Security compromises. If FirstNet has reasonable grounds to believe that Customer Personal Information has been accessed or acquired by an unauthorised person through FirstNet's Admin Access or systems, 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 (assessment reports, configuration documentation and tickets) are held in South Africa by default. Tenant data is processed in the locations Microsoft publishes for its service, as described in Microsoft's terms and the Microsoft Cloud (CSP) Service Specific Terms; where this is outside South Africa, it is processed under the Customer's contract with Microsoft and section 72 of POPIA. Where FirstNet's monitoring tools export Tenant logs to another location named in the Service Schedule, that location is stated there.
- 8.5 Cross-border transfers. FirstNet does not transfer Customer Personal Information outside South Africa for this Service, except to the extent that a tool or location named in the Service Schedule is outside South Africa, in which case the transfer is made under section 72 of POPIA on the basis stated in the Data Processing Annexure.
- 8.6 Exit. At the end of the Service, FirstNet will hand over its documentation of the Baseline, and the Customer must remove FirstNet's Admin Access. Policies remain in the Tenant unless the Customer asks FirstNet to remove them.

9. Fees, licences and changes

- 9.1 The MRC, NRC, project fees and any time-and-materials rates are set out in the Service Schedule. These SST do not state prices.
- 9.2 Managed-service Charges may be based on the number of users or the controls in scope. Changes in user numbers are charged from the next billing cycle.
- 9.3 Work outside the Service Schedule, including remediation of issues found in an assessment, is quoted separately.

10. Term, cancellation and early termination

- 10.1 A project ends when its deliverables are accepted. A managed 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 managed service before the end of the Initial Period, the early termination charges in the Agreement apply, unless the Service Schedule states different charges. If the Customer cancels a project after it has started (other than for FirstNet's breach), the Customer pays for work performed up to the cancellation date, third-party costs FirstNet has committed for the project and cannot recover, and, for fixed-price work, a proportion of the fixed price matching the work completed, 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).

11. Suspension

- 11.1 FirstNet may suspend 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 the Customer's instructions would require FirstNet to act unlawfully or create a serious security risk, or if the law or a competent authority requires it. Suspension does not remove policies already applied to the Tenant.

12. Liability specifics

- 12.1 The limitations and exclusions of liability in the Agreement apply. These SST do not state a separate cap.
- 12.2 Subject to the Agreement, FirstNet is not liable for loss or damage arising from:
- 12.2.1 a user or administrator lock-out, or disruption to users, caused by a policy that the Customer approved, where FirstNet followed the agreed rollout and the Customer did not maintain its Break-Glass Accounts;
 - 12.2.2 data deleted, not retained or not found because of retention, DLP or eDiscovery settings the Customer chose or approved;

- 12.2.3 security incidents in the Tenant that the configured controls did not prevent, where FirstNet provided the Service in accordance with these SST;
- 12.2.4 changes made in the Tenant by the Customer, Microsoft or other providers; or
- 12.2.5 the Customer's failure to implement recommendations, hold required licences or give required notices to its users.

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

13. Regulatory notes

- 13.1 Monitoring of users. Audit logging, DLP, insider-risk and eDiscovery features monitor users' activity and communications. The Customer is responsible for informing its users in advance as required by section 6 of RICA, for a lawful basis and notice under POPIA, and for complying with labour law.
- 13.2 Records and legal holds. The Customer is responsible for deciding retention periods and legal holds under the laws that apply to it (for example the Companies Act, tax legislation and ECTA) and for preserving information when litigation is expected.
- 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 Microsoft's products or 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.
- 14.2 The version number and effective date below identify this version.

Microsoft 365 Security and Compliance | 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. Microsoft 365 Security and Compliance, v2026.10c. The current version of every FirstNet legal document is at www.firstnet.co.za/legal-notices/.