FIRSTNET TECHNOLOGY SERVICES

Rapid Response Services Guide

Client Support, Communication & Escalation Framework

Version 1.4 · Effective 15 June 2026 · Owner: Technical Manager, FirstNet

About this guide
This guide explains how FirstNet supports you — how to reach us, how we prioritise and communicate during incidents, how we escalate, and what you can expect at every stage. It is written to be simple and practical. It does not establish or limit the scope of obligations under your agreement; where product-specific terms apply, those terms govern.

1. How to Reach FirstNet

All service requests are logged and managed through the FirstNet Rapid Response Service Desk. Only registered Technical Contacts (TCs) may log requests. Every request receives a reference number that stays with it for its full life.

A note on terms: an *incident* is an unplanned interruption to a service (an outage or degradation); it is logged and tracked as a *service request*. A service request may also be a change or an access request. The same priorities, response times, and escalation apply throughout.

Logging a Service Request

Use any of the following, in order of preference:

Channel	Contact	Availability
Client Zone (preferred)	clientzone.firstnet.co.za	24×7
Email	support@firstnet.co.za	24×7
Telephone	0861 989 896	24×7

Information to include

To help us respond quickly, please provide: your company name, Technical Contact details, a description of the incident, the business impact, the priority, the affected location or service, and any relevant detail. A full logging template is provided in Section 9.

2. Priorities & First Response Times

Every request is assigned a priority based on its business impact. The priority determines how quickly we respond and how we communicate. First response is measured from the time a request is logged to our first notification or contact with you.

Priority	Definition	First Response
P1 — Critical	Service unavailable or severely degraded; critical business impact; no reasonable workaround.	30 minutes (24×7)
P2 — Major	Service degraded; significant but partial impact.	1 hour (24×7)
P3 — Minor	Minor impact on the business.	6 business hours
P4 — Routine	No impact on the business (e.g. information or routine change).	8 business hours

Note: Priority levels P1–P4 replace the previous Severity 1–4 labels. The definitions and response times are unchanged; the wording is now consistent across all FirstNet client documents.

3. Our Communication Commitments

During a Priority 1 incident you can rely on the following commitments. They are deliberately simple so you always know what to expect from us.

Commitment	What you can expect
Response	We respond to a Priority 1 incident within 30 minutes of it being logged, 24×7.
Updates	We provide proactive status updates at least every 30–60 minutes for the duration of the incident — until your service is restored or the incident is downgraded — even when the update is to confirm that work is ongoing.
Ownership	A single, named owner is accountable for your incident and remains responsible from the moment it is accepted until your service is restored.
Escalation	You can escalate at any time using the contacts provided. We also escalate internally on your behalf at defined intervals, without you having to ask.
Material changes	We tell you immediately of any significant change, new risk, or revised restoration estimate.

4. Service Restored vs Service Resolved

We manage every incident in two clear stages, and we always tell you which stage you are at:

Stage	What it means
Service Restored	The service is operational and available for normal use, although investigation into the underlying cause may continue.
Service Resolved	The underlying cause has been permanently addressed and no further corrective action is required.

5. Major Incident Handling

A Major Incident is a Priority 1 incident with significant or widespread business impact — a critical service is unavailable or severely degraded and no reasonable workaround exists. Examples include:

- A multi-site outage affecting several of your locations at once.
- A national service outage affecting your operations countrywide.
- A data centre outage impacting hosted or core services.
- A widespread network failure affecting connectivity across your business.

When a Major Incident is declared, FirstNet applies its highest level of response. A single accountable owner coordinates the response from start to finish, specialist engineers are engaged immediately, and work continues without interruption until your service is restored.

During a Major Incident you can expect:

- A first response within 30 minutes of logging (24×7).
- Proactive updates at least every 30–60 minutes until your service is restored.
- Immediate notification of any material change or revised restoration estimate.
- A named point of contact for the duration of the incident.

Major Incidents receive increasing management oversight as they continue. Where an upstream provider is involved, FirstNet manages and drives that vendor's escalation on your behalf, giving you a single, consolidated view of progress.

6. Escalation Framework

You may escalate any active request at any time. All escalation timers are measured from the time the request is logged. We also escalate internally on your behalf at the timeframes below — you do not have to ask.

Escalation contacts

When	Escalation contact
Business Hours (Mon–Fri, 08:00–17:00 SAST)	Email: escalations@firstnet.co.za
After Hours (incl. weekends & public holidays)	Telephone: 0861 924 686 (24×7)

Escalation timeframes

Priority	Escalation point(s)	What happens
P1	First: 2 hours · Second: 4 hours	First escalation engages the Escalation Manager; second escalation engages senior management for oversight.
P2	9 hours (24×7)	Escalation Manager engaged to reinforce progress.
P3	18 business hours	Escalation Manager engaged to reinforce progress.
P4	27 business hours	Escalation Manager engaged to reinforce progress.

7. Executive & Management Oversight

> The longer a Priority 1 incident continues, the more management attention it receives. Prolonged incidents are escalated for increasing senior and executive oversight, ensuring the right resources, decisions, and priority are applied until your service is restored. Your most critical incidents always have visibility beyond the team working the fault.

8. Post-Incident Reviews

Following every accepted Priority 1 incident, FirstNet automatically provides a Post-Incident Review — **you do not need to request one**. We deliver a written review within five (5) business days of service restoration. Each review sets out, in plain language:

- What happened and the business impact.
- A timeline of key events, from detection to restoration.
- The identified root cause, or the status of ongoing analysis.
- The corrective and preventive actions we are taking to reduce the likelihood of recurrence.

Post-Incident Reviews are part of our commitment to transparency and to the continuous improvement of the services supporting your business.

9. Service Requests in Detail

Firewall changes

Firewall changes must be authorised by a designated firewall Technical Contact. Specific change processes apply per service.

Scheduled changes

Requests for planned changes that affect business processes should be logged at least 48 hours in advance, so the work can be properly prepared and tested.

Data Centre access

Requests for access to any FirstNet Data Centre must be logged at least 24 hours in advance by a registered TC, to allow for access arrangements (and any upstream requests to Teraco). For emergency access, log the request by phone and email support@firstnet.co.za with the Escalations Manager copied. After-hours access can be facilitated within 1 hour to allow standby personnel travel time. See Section 11.

Fault logging template

Please include the following when logging a fault or information request:

Client information

- Company name
- Technical Contact (TC)
- TC contact telephone number(s)
- TC contact email address (if logging from another address/domain)

Incident details

- Description of the incident
- Priority of the request
- Business impact
- Location address / site name or ID
- Time the incident started
- Actions taken so far

Technical details (if applicable)

- Circuit number / Service ID (network fault)
- Telephone extensions affected (voice fault)
- Hosted services affected (cloud hosting fault)
- Hosted cyber-security platform affected (security fault)
- Attachments — screenshots, files, trace routes, etc.

10. Your Technical Contacts

Registered Technical Contacts (TCs) are central to effective support. Communication with the Rapid Response Service Desk is restricted to authorised TCs, who identify themselves when logging a request. TCs are responsible for:

- Providing first-level support, advice, and guidance to their End Users.
- Initiating and escalating requests to FirstNet as needed (FirstNet may decline requests logged directly by End Users).
- Reporting any detected service deficiency to FirstNet promptly.

- Keeping FirstNet informed of future plans that may affect services.
- Ensuring relevant contacts are subscribed to FirstNet notifications.
- Notifying FirstNet of any change to TC details.

11. Access to FirstNet Data Centres

To keep our Data Centres secure:

- Only designated TCs may log requests for Data Centre (DC) access.
- All equipment entering or leaving a Data Centre must be documented in the related request.
- A separate request must be logged for each visit, stating: DC location; name and ID/passport number of each visitor; date and time of the visit; purpose; and, for after-hours visits, vehicle registration.

On-site arrival

- Umhlanga Data Centre: present the request number and photo ID to the FirstNet engineer.
- Cape Town or Isando Data Centres: present the Teraco request number (provided by FirstNet) and photo ID to the Teraco security desk.

12. Infrastructure Outages & Notifications

If a FirstNet infrastructure outage causes multiple P1 incidents, response aligns with P1 and the event is managed as a Major Incident (Section 5). We promptly notify affected clients and escalate.

FirstNet Notification System

Our Notification System keeps subscribed Technical Contacts informed of network or service outages and of planned and emergency changes. Notifications are categorised as Minor (very low impact), Major (potentially service-impacting), or Critical (service-impacting), and are sent at least every 30–60 minutes during an active event, depending on the services affected.

Governance & Document Control

This framework is issued by FirstNet management and is effective from the date shown. It does not establish or limit the scope of obligations under the underlying agreement.

Field	Detail
Document Owner	Technical Manager, FirstNet Technology Services (Pty) Ltd
Version	1.4
Effective	15 June 2026
Next review	15 June 2027