Annexure A — GNR Connect Acceptable Use Policy (AUP)

1. Introduction & Purpose

This Acceptable Use Policy (AUP) sets out the rules for using services provided by **GNR Connect (Pty) Ltd** ("GNR Connect", "we", "us", "our"). It exists to protect our customers, our network partners' infrastructure and the wider internet community. By using GNR Connect services you agree to comply with this AUP. Non-compliance may result in suspension, restriction or termination of services and/or other remedial steps.

2. Scope

This AUP applies to all services supplied by GNR Connect including, but not limited to:

- FTTH (Fibre to the Home) and FTTB (Fibre to the Business) access;
- Mobile internet and data solutions;
- Managed Wi-Fi and Wi-Fi CCTV / surveillance connectivity services (hardware sold or supported by GNR Connect);
- Any value-added services, portals, APIs or managed network services we provide.

It applies to all subscribers, end-users, devices or systems connected to or using our services.

3. Acceptable Use — General Principles

You must use our services lawfully and responsibly. Acceptable use includes normal personal, business or commercial communications consistent with applicable law, the ISPA Code of Conduct and reasonable network use that does not harm others or the network.

4. Unacceptable Use (examples — non-exhaustive)

The following uses are prohibited. We may act immediately if we reasonably believe any of these are occurring:

4.1 Illegal acts

- Any criminal or unlawful activity, including facilitating, promoting, or attempting to commit crime.

4.2 Harm to the network or others

- Actions that degrade, inhibit or interfere with our ability to provide services to others (for example, launching or participating in DDoS attacks, flooding, excessive bandwidth consumption that overwhelms shared infrastructure, automated port scanning or vulnerability scanning without authorization).
- Unauthorized access, hacking, or attempts to probe or bypass network security.

4.3 Abuse and fraud

- Sending bulk unsolicited commercial electronic messages (spam) in breach of the Electronic Communications and Transactions Act or other applicable laws or the ISPA Code of Conduct.
- Using services to commit fraud, phishing, identity theft or scams.

4.4 Infringing content

- Hosting, distributing or linking to copyrighted material without authorization; or providing file-sharing services in breach of copyright law.

4.5 Malicious software & malware distribution

- Distribution, hosting or control of malware, botnets, ransomware, keyloggers or other harmful code.

4.6 Misuse of CCTV & monitoring services

- Using CCTV systems, recorded imagery, or connected Wi-Fi camera services in a way that violates privacy laws, local regulations, or other persons' rights (e.g., secret surveillance of private spaces, recording without legally required notices/consent).

4.7 Harassment, hate speech, and content that encourages violence

- Using services to threaten, harass, intimidate, or incite others to commit violence or hate crimes.

4.8 Breach of contract or policy

- Any activity that violates other agreements with GNR Connect, upstream providers' policies, or third-party terms of service.

5. Customer Responsibilities

- Keep account details, passwords and devices secure; notify us immediately of any compromise.
- Ensure devices on your network (including ONTs, routers, Wi-Fi access points) are configured securely and kept up to date.
- Obtain lawful consent where required for recording or monitoring (CCTV, voice, data capture).
- Follow any reasonable directions from us to mitigate an incident or to protect the network.

6. Monitoring, Enforcement & Remediation

- We may monitor usage to the extent permitted by applicable law to protect the network and detect violations. Monitoring is limited to what is reasonably necessary for network security, abuse prevention and service quality.
- If we reasonably suspect a breach of this AUP we may: notify you, throttle or restrict specific traffic, block offending traffic, suspend individual services or accounts, or terminate services in serious or repeated cases.
- We may disclose relevant information to law enforcement, upstream providers or affected parties as legally required or to prevent imminent harm.

7. Reporting Abuse or Security Incidents

To report abuse, security incidents, suspicious traffic, or breaches of this AUP please contact us:

- **Abuse/security:** info@grconnect.co.za
- **Support / general queries:** support@grconnect.co.za
- **Compliance / policy appeals:** gopolang@grconnect.co.za
- **Phone:** 072 884 3383

When reporting, please include relevant details (time, IP address, screenshots or logs where available) to help investigation and remediation.

8. Suspension & Notice Procedures

- Where possible we will notify account holders of alleged breaches and give an opportunity to remediate. However, we reserve the right to act immediately in cases of serious abuse or where delay would cause material harm (for example a live DDoS or ongoing data exfiltration).
- Notices will be sent to the primary account email or other contact methods on file.

9. Appeals & Dispute Resolution

If you believe action taken against your account was incorrect, contact info@grconnect.co.za with evidence and a clear statement of why the decision should be reconsidered. We will review and respond within a reasonable timeframe.

10. Legal & Regulatory Compliance

- You must comply with all applicable South African laws (including ECT Act, POPIA where personal data is involved, and other applicable privacy and telecommunications laws) and the ISPA Code of Conduct where relevant.
- For services we resell or deliver under upstream partner agreements, you must also comply with any specific terms that apply to those services.

11. Changes to this AUP

We may update this AUP from time to time. We will publish the revised AUP on our website and use reasonable means (email or customer portal notice) to let you know of material changes.

12. Definitions (brief)

- **Service(s):** Any connectivity, data, managed Wi-Fi, CCTV connectivity or other products supplied by GNR Connect.
- **User/Customer:** The person or entity subscribing to or using our services.
- **Abuse:** Activity that contravenes this AUP, harms the network, or violates law or contract.

13. Contact & Company Details

GNR Connect (Pty) Ltd
2019/530068/07
6802 Mirt Place, 2622 Valley View Estate, 501 Rooihuiskraal Rd, Kosmosdal, Samrand, Centirion, 0157
Email: info@grconnect.co.za

Approval

This Acceptable Use Policy is issued by GNR Connect management and forms part of the contractual terms for use of our services.