INFORMATION REGULATOR
(SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

Address: JD House, 27 Stiemens Street
Braamfontein, Johannesburg, 2001
P.O. Box 31533
Braamfontein, Johannesburg, 2017
Email: Enquiries@inforegulator.org.za
Tel: 010 023 5200

SUPPLY CHAIN MANAGEMENT SPECIFICATION	
Name of Directorate	Information Regulator
Date of Specification	21 May 2025
Closing Date	**28 May 2025**
Contact Number	010 023 5200
Venue for delivery of goods / services	54 Maxwell Drive Woodmead, Midrand, 2191
Contact E-mail and Fax	scm@inforegulator.org.za
Contact Person	Lesego Korae / Kido Lofafa / Phindulo Maphangula

SPECIFICATION FOR THE PROVISION OF HIGH-SPEED INTERNET CONNECTIVITY AND SECURE WI-FI SERVICES, INCLUDING SUPPORT AND MAINTENANCE, TO THE INFORMATION REGULATOR FOR A PERIOD OF TWO YEARS. (01 JULY 2025 – 30 JUNE 2027)

Specification to be supplied	**Qty**	**Description**
1) High-speed fibre internet connectivity. **2) Secure Wi-Fi configuration.** **3) Support and Maintenance.**		**Refer to Page 2**

1. INTRODUCTION

The Information Regulator (South Africa) seeks to appoint a capable and experienced Internet Service Provider (ISP) to deliver high-speed, enterprise-grade internet connectivity and secure Wi-Fi infrastructure for a period of 24 months, commencing 1 July 2025. The Regulator operates a hybrid ICT architecture that heavily depends on cloud-hosted services (Microsoft 365, Exchange Online, SharePoint Online, Veeam Cloud, Azure Active Directory, and SendGrid), as well as critical on-premises systems. The required service must support high availability, speed, security, and full compatibility with existing cloud-based applications, while also including the setup, support, and maintenance of a secure Wi-Fi environment.

2. OBJECTIVE

To provide a scalable, secure, and cloud-optimized internet and Wi-Fi service that guarantees seamless and uninterrupted access to essential platforms and applications, especially those hosted in the cloud, while also maintaining internal connectivity, remote access, VoIP services, and endpoint integration through the Regulator’s Fortinet security infrastructure. The service must include comprehensive support and maintenance throughout the 24-month contract period.

3. TECHNICAL REQUIREMENTS

3.1 Connectivity Type

- Dedicated Fibre-to-the-Business (FTTB) line with:
    - 500 Mbps synchronous bandwidth (upload/download) as the primary link.
    - 100 Mbps synchronous failover link, routed separately or through wireless/fibre alternate path.
- Uncontended 1:1 connection with enterprise-grade SLA.
- Latency to major local cloud regions (Azure South Africa North/South) must not exceed 10ms.

3.2 Cloud Application Access Optimisation

- Direct and optimised routing to major cloud providers, including:
    - Microsoft Azure (South Africa North and South regions).
    - Microsoft 365 workloads (Exchange Online, Teams, SharePoint Online).
    - SendGrid Email API, Veeam Backup for Microsoft 365, and Azure AD/Entra ID.
- Maintain peering agreements or direct interconnects with cloud providers to minimise hops and latency.
- Ensure zero international routing for services hosted in South Africa-based cloud data centres.
- Support quality of service and bandwidth prioritisation for:
    - Microsoft Teams
    - OneDrive and SharePoint sync
    - Email backup/upload/download
    - Veeam backup to cloud
    - Secure authentication and token requests to Entra ID

3.3 IP Addressing

- Minimum of 300 static public IPv4 addresses, with full route control and BGP (Border Gateway Protocol) support for dynamic routing.
- Option to provision IPv6 addresses where required.
- Ability to configure reverse DNS (PTR) records for hosted services and mail systems.
- ISP must support IP address routing for internal network segmentation and traffic management.
- Dynamic Host Configuration Protocol (DHCP) must be provided for seamless IP assignment to user workstations and general endpoint devices

The ISP must accommodate static IP configurations for:

- Internal and public-facing servers,
- Core networking equipment (e.g., firewalls, switches),
- Access points, cloud backup appliances, and other critical infrastructure.

ISP must work with the Regulator’s ICT unit to implement and document a well-structured IP addressing scheme.

3.4 Domain Name Services (DNS)

- Primary and secondary redundant DNS servers.
- Support for internal record delegation and custom DNS zones.
- DNS service must be highly available, with failover capabilities and global propagation support.

3.5 Failover and Redundancy

- Secondary 100 Mbps failover link (licensed microwave, alternate fibre, or LTE Advanced).
- Automatic failover routing using BGP or intelligent routing policy.
- Support for health check-based route switching to maintain service continuity.

3.6 Fortinet Firewall Integration

- Internet handoff must integrate directly with the Regulator’s Fortinet FortiGate firewall.
- ISP must:
    - Work with ICT staff to implement the required bridge or routed mode configuration.
    - Avoid any ISP-enforced NAT/firewalling that conflicts with internal Fortinet policies.
    - Allow FortiGate to manage internet traffic filtering, IPS, antivirus, and application control with full visibility.

3.7 Security Features

- Built-in DDoS mitigation.
- ISP to provide threat monitoring and alerting at the network layer.
- Connection must support:
    - IPSec VPN passthrough.
    - SSL VPN tunnels.
    - GRE/IP-in-IP tunnels for site-to-site access.
- ISP must assist with configuration to maintain compliance with cybersecurity policies.

4. SECURE WI-FI REQUIREMENTS

The service provider will be required to reconfigure eight (8) existing Aruba Instant On access points currently in use by the Regulator, and supply and configure an additional eight (8) enterprise-grade access points.
The ISP must provide, set up, and configure all hardware and software components related to secure Wi-Fi service, including but not limited to:

- A cloud-based Wi-Fi controller with:
    - Central management of SSID profiles and access point provisioning.
    - Admin access to be granted to three ICT staff from the Regulator.
    - Remote monitoring and control capabilities.
    - Create and configure a corporate Wi-Fi Profile that integrates with Entra ID.
    - Create and configure a Guest user profile that is separate from Entra ID.
    - Training on Wi-Fi controller usage for three ICT staff.

    Enterprise-grade access POE switch with:
    - VLAN configuration to separate management, internal access, and guest traffic.
    - Integration with the Fortinet firewall, where applicable.
    - Port configuration for all access points.
    - Port configuration for all six network points.

- Cabling and installation:
    - Cabling for all sixteen (16) access points.
    - Switch cabinet and brush panels where required.
    - Clear, weather-resistant labelling for all cabling and access points.

- Additional network setup:
    - Installation, configuration, and testing of six (6) additional network points within the office premises.

- A compulsory site inspection at the new offices (54 Maxwell Drive, Woodmead) will be required to assist the potential service provider with accurate pricing.

- All installation and commissioning will occur at 54 Maxwell Drive, Woodmead.

5. MONITORING, REPORTING, AND SUPPORT

- The Service must include:
    - Technical support.
    - Detailed network diagram and solution documentation.
    - Access to a dedicated account manager and escalation contact.
    - Monthly reports including:
        - Bandwidth usage.
        - Uptime statistics.
        - Security alerts or threats.
        - Packet loss and jitter.
- The ISP must provide a web-based monitoring portal for real-time visibility of internet usage and performance.

6. IMPLEMENTATION TIMELINE

- Site inspection and survey: Within 5 working days of appointment.
- Installation, configuration, testing, and final handover: By 30 June 2025.

- Go-live date: 1 July 2025.
- The ISP must support traffic simulation and verification tests, including Fortinet integration and Wi-Fi deployment.

ADDITIONAL REQUIREMENTS:

- Detailed pricing for the project, with a clear breakdown of costs.
- At least two (2) references where the service provider has successfully delivered similar services.
- ISP must be ICASA-licensed and comply with all relevant South African cybersecurity and data privacy laws.
- Assignment of a dedicated relationship manager is mandatory.

- ISP must participate in quarterly service review meetings and cooperate with any performance or compliance audits initiated by the Regulator.

Quotation(s) must be accompanied by the following documents, where applicable:

1 Valid Tax Clearance Certificate.
2 Original certified BBBEE Certificate/Sworn Affidavit.
3 Most recent CSD registration report.
4 Quotations must remain valid for two (2) months.
5 Quotations not compliant with the above requirements or received after the specified closing date will NOT be considered.

SPECIFICATION SIGNED OFF BY	
Name	**Mr T. Luyaba**
Position	**Chief Information Officer (CIO)**
DocuSigned by: DFAC8CCA4EE546B... *Signature*	22-May-2025 | 15:21 SAST *Date*