



**SERVICE LEVEL AGREEMENT ENTERED
INTO BY AND BETWEEN**

SEDIBENG DISTRICT MUNICIPALITY herein represented by
MOTSUMI MATHE in his capacity as the Municipal Manager, duly authorised thereto,
(hereinafter referred to as "Sedibeng");

AND

VPN TECHNOLOGIES, CC Registration number CK1999/012869/23 herein
represented by **JACO LANGE** in his capacity as Managing Member (hereinafter
referred to as "the Service Provider").

WHEREAS Sedibeng advertised during November 2023 for interested Service Providers to tender
for the supply of specialist ICT services for website hosting, bandwidth and firewall services to the
Sedibeng District Municipality, Bid no: 8/2/2/13-2023 (hereinafter referred to as "the Services");

AND WHEREAS Sedibeng has, after due supply chain processes awarded the bid to the Service
Provider under certain conditions;

AND WHEREAS the Service Provider has accepted such appointment with the terms and conditions
herein recorded.

NOW THEREFORE IT IS HEREBY AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

1.1 In this agreement, unless clearly inconsistent with or otherwise indicated by the context:

1.1.1 "The/this agreement" means the agreement set out in this document and all
referred to and annexed addenda thereto;

1.1.2 "Date of signature" means the date of signature of this document;

[Handwritten signatures and initials]
M.O.
1

- 1.1.3 **"Effective date"** means that date upon which the last party hereto signs this agreement;
- 1.1.4 **"Equipment"** means any goods or equipment that are supplied to Sedibeng in terms of this Agreement and as stipulated in Annexure "A";
- 1.1.5 **"Parties"** means Sedibeng and the Service Provider jointly;
- 1.1.6 **"Party"** means any one of them as the context may indicate;
- 1.1.7 **"Services"** means the services set out in the Specification;
- 1.1.8 **"Service Charges"** means the fees due to the Service Provider for the services;
- 1.1.9 **"The Service Provider"** means the Service Provider appointed in terms of this agreement; and
- 1.1.10 **"The Panel"** means the list of service providers procured by Sedibeng for purposes of supplying printer cartridges to Sedibeng;
- 1.1.10 Any reference to the singular includes the plural and vice versa;
- 1.1.11 Any reference to natural persons includes legal persons and vice versa; and
- 1.1.12 Any reference to one gender includes the other gender.
- 1.2 Where applicable, the provisions of the above shall impose substantive obligations on the parties as provided in the provisions concerned.
- 1.3 The clause headings in this agreement have been inserted for convenience only and shall not be taken into account in its interpretation.
- 1.4 Words and explanations defined in any sub clause shall, for the purposes of the clause of which that sub clause forms part, bear the meaning assigned to such words and explanations in that sub-clause.
- 1.5 This agreement shall be governed by and construed and interpreted in accordance with the Laws of the Republic of South Africa.
- 1.6 Unless the agreement specifies otherwise:
- 1.6.1 If either party is required to notify the other in terms of this agreement, such notification shall be of no force or effect unless reduced to writing; and
- 1.6.2 Any notices to be furnished by either party shall be delivered in a timely manner and without delay but in any event not later than 30 (thirty) days after being required to do so in terms of this agreement.

2. APPOINTMENT

Sedibeng hereby appoints the Service Provider, which accepts the appointment, to provide firewall, web hosting, bandwidth and network management as specified in clause 5 of this agreement.

3. DURATION

- 3.1 This agreement will commence on the date of signature, and will, subject to the provisions of this agreement, continue to be in force and effect for a period of three (3) years, renewed yearly, based on an annual performance assessment as per terms of reference within the original tender document.

4. SERVICES AND CHARGES

- 4.1 The payment schedule is attached as Annexure "A";
- 4.1.1 In summary payments will be made as follows:

Service provider	Year 1		Year 2		Year 3	
	Frequency	VPN	Frequency	VPN	Frequency	VPN
Firewall hardware (once-off)	1	148,842.00	-	-	-	-
Wi-fi router (once-off)	1	3,899.00	-	-	-	-
Provisioning of bandwidth	12	188,772.00	12	188,772.00	12	188,772.00
Management, monitoring and reporting fees	12	4,800.00	12	4,800.00	12	4,800.00
Proxy traffic analyser	12	7,800.00	12	7,800.00	12	7,800.00
Netflow collector and analyser	12	7,800.00	12	7,800.00	12	7,800.00
Management, monitoring and reporting fees	12	7,800.00	12	7,800.00	12	7,800.00
Web hosting service	12	30,060.00	12	30,060.00	12	30,060.00
Provisioning of mail scanning service	12	175,080.00	12	175,080.00	12	175,080.00
High availability cluster	12	0.12	12	0.12	12	0.12
Management, monitoring and reporting fees	12	4,800.00	12	4,800.12	12	4,800.12
Firewall software provisioning and support	12	15,600.00	12	15,600.00	12	15,600.00
High availability cluster	12	3,600.00	12	3,600.00	12	3,600.00
Firewall standard installation and maintenance	12	7,800.00	12	7,800.00	12	7,800.00
User identity management (LDAP)	12	7,800.00	12	7,800.00	12	7,800.00
Backup, recovery and reconfigurations	12	3,600.00	12	3,600.00	12	3,600.00
Management, monitoring and reporting fees	12	7,800.00	12	7,800.00	12	7,800.00
Data routing, DHCP and DNS protocols	12	150,000.00	12	150,000.00	12	150,000.00
Provisioning and management of VPN	12	7,800.00	12	7,800.00	12	7,800.00
Wireless provisioning, support and reporting	12	7,800.00	12	7,800.00	12	7,800.00
Anti-virus software (450 seats, 10 servers)	1	174,800.00	1	174,800.00	1	174,800.00
Training, support and quarterly visits	4	19,200.00	4	19,200.00	4	19,200.00
SSL licensing, installation and support	1	5,918.00	1	5,918.00	1	5,918.00
Subtotal		991,371.12		838,630.24		838,630.24
VAT		148,705.67		125,794.54		125,794.54
Total		1,140,076.79		964,424.78		964,424.78

	Year 1	Year 2	Year 3	Total (inclusive of VAT)
VPN	1,140,077	964,425	964,424.78	3,068,926.34

Figures correlate with original tender documents submitted and included in Annexure "A"; and

- 4.1.2 The fees payable for the services rendered shall be subject to an annual escalation in accordance with the inflation rate.
- 4.2 Payment for services rendered shall be effected within a period of thirty (30) days of presentation of an invoice to a duly authorized employee of the Customer who shall certify that the amount claimed and the services that are reflected as having been rendered are true and correct.
- 4.3 Payment for the services rendered shall be effected by the Customer directly into the bank account of the Service Provider, which has the following particulars:

Bank Name : ABSA
 Branch Name : Menlyn Park
 Branch Code : 335 645
 Account Name : VPN Technologies CC
 Account Number : 4059139721

[Handwritten signatures and initials]
 M-O
 3

5. SERVICE PROVIDER's RESPONSIBILITIES:

The Service Provider shall provide the following:

5.1. Firewall hardware

5.1.1. Provide and install a Dell PowerEdge R250 Server with the following specifications:

- 5.1.1.1. Intel Xeon E-2314 2.8GHz, 8M Cache, 4C/4T, Turbo (5W)
- 5.1.1.2. 4 x Dell 32GB - 2RX8.DDR4 UDIMM 3200MHz ECC)
- 5.1.1.3. 3 x Dell 960GB SSD SATA Mix Use 6Gbps 512e 2.5in
- 5.1.1.4. Broadcom 5720 Dual Port 1Gb On-Board LOM
- 5.1.1.5. 3 Year Basic Warrant

5.2. High-speed dual band Wi-Fi router

5.2.1. Provide and install an Ubiquiti Access point UniFi AC Pro Wi-Fi router

5.3. Provisioning of bandwidth:

5.3.1. Alternative fibre routing provisioning (current connectivity setup via existing DFA link)

5.3.1.1. Propose and provide an alternative route via another reputable last mile bandwidth provider to ensure redundancy and enhanced reliability;

5.3.1.2. Ensure seamless integration of this alternative route with the existing infrastructure, minimizing potential downtime during the transition.

5.3.2. Functionality and efficient response times

5.3.2.1. Ensuring the consistent and optimal functioning of the provided bandwidth;

5.3.2.2. Guaranteeing a response time (specific time to be defined) for any issues or concerns related to bandwidth or connectivity;

5.3.2.3. Implementing monitoring tools to proactively detect and address any potential disruptions.

5.3.3. Reporting of faulty data lines

5.3.3.1. Continuously monitor the health and performance of all data lines;

5.3.3.2. Rapidly switching lines between alternative routing paths to ensure high uptime;

5.3.3.3. Promptly reporting any faults or disruptions to the service provider, ensuring swift resolution and minimal impact on operations.

5.3.4. Recreating ports

5.3.4.1. Managing and monitoring all network ports associated with the provided bandwidth;

5.3.4.2. Recreating and reconfiguring ports as necessary, especially in the event of failure or changes in the network topology.

[Handwritten signatures and initials]
M-D
4

5.3.5. Troubleshooting internet connection failures

- 5.3.5.1. Providing immediate basic troubleshooting in the event of any internet connection failures;
- 5.3.5.2. Collaborating with the fibre providers and internal ICT staff members to ensure swift resolution of any connectivity issues.

5.3.6. Monthly performance reporting

- 5.3.6.1. Producing detailed monthly reports on bandwidth performance, usage patterns, and any detected issues;
- 5.3.6.2. Providing insights and recommendations based on these reports, ensuring Council remains informed and can make data-driven decisions regarding its digital infrastructure.

5.3.7. Additional inputs

- 5.3.7.1. Bandwidth is an essential tool in Council's ICT infrastructure. By emphasizing the provisioning of bandwidth and ensuring redundancy and reliability, Sedibeng District Municipality can maintain a high-performing and resilient digital infrastructure. The section above provides a detailed overview of the services required for bandwidth provisioning.
- 5.3.7.2. Depending on the specific needs and requirements of the council, additional details, terms, and conditions may be necessary.

5.4. Analysis of internet traffic

5.4.1. Squid proxy traffic analyser

- 5.4.1.1. Provision of a a lightweight, swift, web-based squid proxy traffic analyser;
- 5.4.1.2. Ensuring the tool effectively examines access logs to generate detailed reports on a per-user and per-group basis;

5.4.2. NetFlow collector and analyser

- 5.4.2.1. Providing a robust NetFlow collector and analyser tool suitable for troubleshooting and detailed traffic analysis;
- 5.4.2.2. Providing for the retention of data for a minimum of seven (7) days, allowing for historical analysis and review;
- 5.4.2.3. Assisting in any issues related to the setup, usage, or troubleshooting of the NetFlow tool.

5.4.3. Monthly reporting

- 5.4.3.1. Delivering comprehensive monthly reports detailing the performance, user activity, and any notable trends observed from the analysed data;
- 5.4.3.2. Highlighting any potential concerns or anomalies that may require attention or action.

 m.o
5

5.5. Web hosting services

5.5.1. Domain hosting and technical support

- 5.5.1.1. Hosting of the Sedibeng domain on reliable servers;
- 5.5.1.2. Providing prompt and efficient technical support to address any issues or queries related to web hosting;
- 5.5.1.3. Ensure that a dedicated team or representative is available for support, especially during critical business hours;
- 5.5.1.4. Managing and maintaining the webserver's Content Management System (CMS) to ensure smooth operations and updates;
- 5.5.1.5. Overseeing the webserver's operating system, ensuring it is up-to-date and patched against known vulnerabilities;
- 5.5.1.6. Implementing robust security measures to protect the webserver and hosted content from potential threats, breaches, or cyber-attacks;

5.5.2. Secure socket layer security protocol requirements

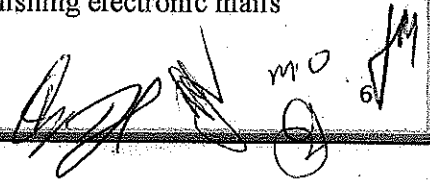
- 5.5.2.1. Ensuring that the hosted website is secured using Secure Socket Layer (SSL) to encrypt data transmission between the server and users;
- 5.5.2.2. Facilitating the timely renewal of the SSL certificate and ensure that it remains valid and trustworthy;
- 5.5.2.3. Installing valid SSL certificates on the necessary servers and platforms, ensuring a seamless and error free process;
- 5.5.2.4. Addressing any compatibility of installation issues promptly, ensuring uninterrupted encrypted connections for users;
- 5.5.2.5. Assist in any issues related to SSL installation, renewal, or troubleshooting.

5.6. Mail scanning (electronic mail services)

5.6.1. Provisioning of mail scanning services (automatically review electronic mail messages for viruses, malware, and spam)

- 5.6.1.1. Deploying a mail scanning service on-site, ensuring the service acts as the primary relay between the mail server and the internet;
- 5.6.1.2. Configuring the gateway to scan all incoming and outgoing emails, ensuring no malicious content bypasses the system;
- 5.6.1.3. Setting up service in a high availability (HA) cluster configuration to ensure an uninterrupted mail scanning services is provided;
- 5.6.1.4. Ensure that in the event of a node failure, another node in the cluster automatically takes over, guaranteeing seamless service availability.

5.6.2. Blocking of unsolicited messages (spam), viruses and phishing electronic mails

Handwritten signatures and initials, including "MO" and "6", are present at the bottom right of the page.

- 5.6.2.1. Utilizing advanced spam detection mechanisms to filter out unwanted emails;
- 5.6.2.2. Ensuring real-time virus scanning;
- 5.6.2.3. Implementing phishing detection to block scam emails that might deceive users.

5.6.3. Domain management

- 5.6.3.1. Blocking or whitelisting specific domains as per the organization's requirements;
- 5.6.3.2. Promptly act (two (2) hour window period) on requests to release emails mistakenly caught by the filters or to block specific senders.

5.6.4. Setup, updating and recovery

- 5.6.4.1. Regularly monitor for software updates and patches and apply updates in a timely manner, ensuring the system benefits from the latest security patches and features;
- 5.6.4.2. Reloading or reconfigure the service to its optimal settings when required, ensuring minimal downtime during this process.

5.6.5. Monthly management reports

- 5.6.5.1. Providing comprehensive monthly management reports detailing the number of emails processed, blocked spam, detected viruses, and phishing attempts etc.
- 5.6.5.2. Furnishing insights into any emerging threats or patterns observed in the email traffic.

5.7. Firewall services:

5.7.1. Provisioning and support

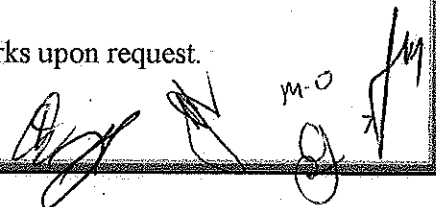
- 5.7.1.1. Supplying firewall server and software;
- 5.7.1.2. Configuring firewall aligned with SDM's requirements;
- 5.7.1.3. Daily maintenance of the firewall server and software to guarantee performance;
- 5.7.1.4. Timely applying updates and patches to the firewall software;
- 5.7.1.5. Providing high availability (HA) cluster to guarantee continuous service as well as providing switch gear to oversee the failover process.

5.7.2. User identity management with lightweight directory access protocol (LDAP) integration:

- 5.7.2.1. Offering a robust system for user identity management, ensuring secure access and monitoring of user activities on the network;
- 5.7.2.2. Ensuring seamless integration with LDAP for centralized authentication and authorization.

5.7.3. Uniform resource allocator (URL) and website blocking:

- 5.7.3.1. Blocking specific URLs, websites, and social networks upon request.



5.7.4. Data backup:

- 5.7.4.1. Conducting daily backups of the firewall software and data;
- 5.7.4.2. Guaranteeing the secure storage of backups and rapid restoration.

5.7.5. Recovery and setup:

- 5.7.5.1. As and when required promptly reload the firewall software;
- 5.7.5.2. Reconfiguring of firewall to ensure optimal performance.

5.7.6. Port management:

- 5.7.6.1. Opening specific ports when requested, balancing between operational needs and security.

5.7.7. Monthly reporting;

- 5.7.7.1. Providing monthly reports and assessments detailing the firewall's performance;
- 5.7.7.2. Documenting security threats or breaches detected, along with proof of remedial actions executed.

5.7.8. Bandwidth provision and support:

- 5.7.8.1. Provisioning a firewall capable of supporting bandwidth throughput of at least 1 Gigabyte per second (Gb/s).

5.7.9. Fault reporting and change control management:

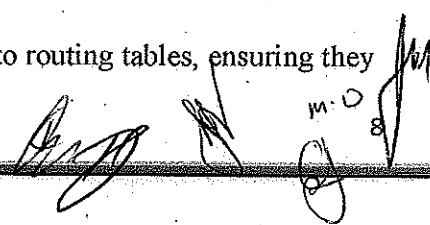
- 5.7.9.1. Operate a dedicated helpdesk for addressing firewall-related inquiries or issues;
- 5.7.9.2. Establish a stringent change control procedure, ensuring all alterations to the firewall configuration are documented, sanctioned, and don't jeopardize the firewall's availability.

5.8. Routing of data, DHCP and DNS protocol management

5.8.1. Network setup, routing and troubleshooting

- 5.8.1.1. Assisting the organization in setting up the network infrastructure, ensuring efficient routing of data across all devices and systems;
- 5.8.1.2. Addressing and troubleshooting any network performance issues promptly (two (2) hour response time), ensuring minimal downtime;
- 5.8.1.3. Supporting in the integration of new IP subnets into the existing network; ensuring seamless connectivity.

5.8.2. Routing table management and support

- 5.8.2.1. Overseeing and maintaining the routing tables, ensuring data is routed efficiently and securely throughout the network;
 - 5.8.2.2. Provide support for any issues or concerns related to routing tables, ensuring they are consistently optimized for performance.
- 

5.8.3. Network switch management and traffic optimization

- 5.8.3.1. Managing and monitoring network switches, ensuring they operate at peak performance and reliability;
- 5.8.3.2. Optimizing network traffic and routing, ensuring efficient data transmission and minimizing potential bottlenecks.

5.8.4. Performance reviews on routing

- 5.8.4.1. Conducting regular reviews and assessments on the efficiency and effectiveness of data routing within the organization's network;
- 5.8.4.2. Providing actionable insights and recommendations to enhance routing performance and security.

5.8.5. Expansion and updating of tables

- 5.8.5.1. Regularly updating and expanding routing tables to accommodate network growth, changes, and evolving needs;
- 5.8.5.2. Ensuring that the routing tables are adjusted and optimized to maintain peak performance as the organization's network evolves.

5.8.6. DHCP and DNS protocol management

- 5.8.6.1. Overseeing and managing the Dynamic Host Configuration Protocol (DHCP), ensuring devices within the network receive IP addresses efficiently and without conflicts;
- 5.8.6.2. Managing the Domain Name System (DNS) protocols, ensuring domain name resolutions are accurate, swift, and secure;
- 5.8.6.3. Addressing and resolve any issues or anomalies related to DHCP and DNS, ensuring consistent network operations.

5.9. Provisioning and management of virtual private network (VPN)

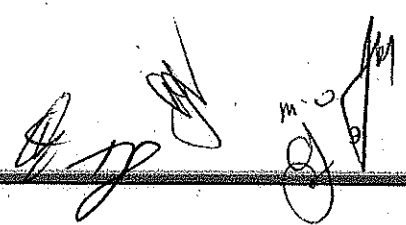
5.9.1. VPN for remote sites

- 5.9.1.1. Provisioning and setting up VPN connections for remote sites, ensuring they have secure and reliable access to the central network;
- 5.9.1.2. Monitoring and maintaining these connections, ensuring consistent uptime and addressing any connectivity issues promptly.

5.9.2. VPN links for off-site users

- 5.9.2.1. Establishing VPN links that allow off-site users, such as remote employees or partners, to securely connect to the customer's network;
- 5.9.2.2. Ensure that these links are easy to use, reliable, and provide a seamless user experience.

5.9.3. VPN certificate management



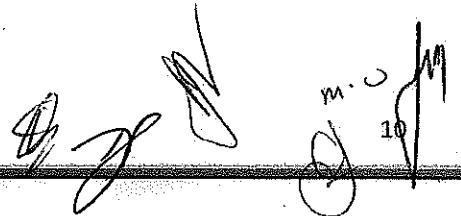
- 5.9.3.1. Generating and managing VPN certificates necessary for authentication;
- 5.9.3.2. Rendering assistance to users in installing and configuring these certificates, ensuring they can securely connect to the VPN without issues.
- 5.9.4. Advanced encryption for data security
 - 5.9.4.1. Utilizing the most advanced encryption standards and protocols available to secure data transmission through the VPN;
 - 5.9.4.2. Regularly reviewing and updating encryption methods in line with industry best practices and emerging threats.
- 5.9.5. Monthly access and usage reports
 - 5.9.5.1. Producing comprehensive monthly reports detailing VPN access patterns, usage statistics, and any security events;
 - 5.9.5.2. Providing insights into user behaviour, peak usage times, and any potential areas of concern or improvement.

5.10. Wireless networking technology provision and management (Wi-Fi)

- 5.10.1. Recommending and providing high-speed dual-band Wi-Fi routers (hardware) when required;
- 5.10.2. Setting up of hardware and managing access control;
 - 5.10.2.1. Professionally installing and configuring the equipment, ensuring optimal signal strength and coverage throughout the designated areas;
 - 5.10.2.2. Setting up a secure wireless network, segregating public access from internal networks to maintain security;
 - 5.10.2.3. Implementing access control measures, such as captive portals, where users may need to authenticate or accept terms of service before gaining access;
 - 5.10.2.4. Monitoring and managing connected devices, ensuring bandwidth is fairly distributed and no single device monopolises the network.
 - 5.10.2.5. Regularly updating the firmware of the equipment to ensure devices are protected against known vulnerabilities and benefit from the latest features.

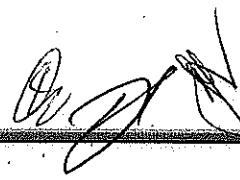
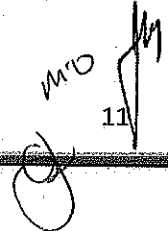
5.11. Providing anti-virus software and support

- 5.11.1. Providing comprehensive anti-virus and anti-spyware software (450 user and 10 server licenses), with the following features
 - 5.11.1.1. Eliminate all types of threats, including viruses, rootkits, worms and spyware;
 - 5.11.1.2. Be a host-based intrusion prevention system;
 - 5.11.1.3. Contain an exploit locker;
 - 5.11.1.4. Monitor the behaviour of malicious processes;



Handwritten signatures and initials at the bottom right of the page, including a large signature and the number 10.

- 5.11.1.5. Effectively filters out spam and scans all incoming emails for malware;
- 5.11.1.6. Place low system demands on hardware;
- 5.11.1.7. Protect end-users from fake websites etc. (anti-phishing);
- 5.11.1.8. Provide botnet protection;
- 5.11.1.9. Allow for device control, blocking unauthorised devices (i.e. CDs/DVDs/USBs);
- 5.11.1.10. Allow for a local update server;
- 5.11.1.11. Facilitate easy management through a user-friendly administrator tool;
- 5.11.1.12. First installation date March 2025;
- 5.11.1.13. Ensure continuity of protection by renewing the organization's subscription in a timely manner.
- 5.11.2. Software roll-out assistance
 - 5.11.2.1. Assisting in the deployment of the anti-virus software on both remote and local devices, ensuring all devices are adequately protected;
 - 5.11.2.2. Addressing any installation or compatibility issues promptly, ensuring a smooth roll-out process.
- 5.11.3. Training and skills transfer
 - 5.11.3.1. Providing comprehensive training sessions to ICT staff and end-users on the effective use and management of the anti-virus software;
 - 5.11.3.2. Transferring essential skills to the organization's ICT team, ensuring the independent management and troubleshooting of the software.
- 5.11.4. Quarterly site visits
 - 5.11.4.1. Conducting quarterly site visits to assess the software's performance, address any concerns, and provide on-site support;
 - 5.11.4.2. Engage with ICT staff during these visits to discuss any potential improvements or updates.
- 5.11.5. Patch distribution monitoring and support
 - 5.11.5.1. Monitoring and supporting the distribution of patches and updates for the anti-virus software, ensuring all devices have the latest security definitions;
 - 5.11.5.2. Addressing any issues related to patch distribution promptly, ensuring consistent protection across all devices.
- 5.11.6. Local management and monitoring tools
 - 5.11.6.1. Providing tools that allow the organization's ICT team to manage and monitor the anti-virus software locally;



11

- 5.11.6.2. Ensuring these tools are user-friendly and provide comprehensive insights into the software's performance and security events.

5.11.7. Monthly Reporting

- 5.11.7.1. Producing detailed monthly reports that cover the distribution of the software, any exceptions encountered, and occurrences of detected threats;
- 5.11.7.2. Providing insights and recommendations based on these reports, ensuring the organization remains informed and proactive in its approach to device security;

5.12. Management and performance reviews

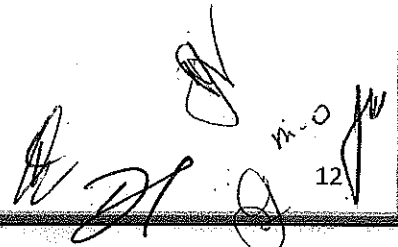
- 5.12.1. Conducting monthly performance meetings with the organization's ICT team and relevant stakeholders. The cost of these meetings should be included in the support fees;
- 5.12.2. Addressing any concerns, provide updates, and discuss potential improvements during these meetings;
- 5.12.3. Delivering comprehensive monthly reports detailing network performance, internet usage and security events on or before the 5th of each month;
- 5.12.4. Preparing actionable insights and recommendations based on these reports, ensuring proactive measures are taken to maintain optimum performance and security; and
- 5.12.5. Allocate a specified amount of hours each quarter dedicated to skills transfer. Ensure that during these sessions, essential skills, knowledge, and best practices are transferred to the organization's ICT team. Customize these sessions based on the organization's needs, ensuring maximum value and empowerment.

5.13. Additional items to the contract

- 5.13.1. During the duration of the contract, additional items may be added to the contract. New items will be quoted on, a market related benchmark will be performed and a recommendation will be made to the Supply Chain Management (SCM) Department to include the items in the current contract.

6. SEDIBENG's RESPONSIBILITIES:

- 6.1 Pay the amounts due to the Service Provider timeously and in the manner described in clause 4 above;
- 6.2 Provide all the necessary information and support to the Service Provider that is reasonably necessary to enable the service provider to efficiently render services; and
- 6.3 Designate a project manager to liaise with the Service Provider in matters pertaining to this agreement.

 12

7. LIABILITY

- 7.1 The Service Provider shall be liable for any damages sustained by Sedibeng as a result of breach of contract or negligence on its part in respect of the services. The maximum liability of the service provider for all claims arising out of the services provided in connection with this agreement shall be limited to an amount equal to twice the monthly fees for the services as set out in clause 4 above.
- 7.2 The Service Provider shall be liable for direct damages or losses incurred by third parties arising from its proven gross negligence or wilful misconduct in the performance of its obligations under this agreement. Liability for such third-party claims shall not exceed the limitation set out in clause 7.1.

8. TERMINATION AND BREACH

- 8.1 In the event that any party ("the defaulting party") commits a breach of any of the provisions of this agreement, the other party ("the aggrieved party") may give the defaulting party seven (7) days written notice to remedy such breach.
- 8.2 Should the defaulting party fail to comply with such notice, the aggrieved party shall be entitled to cancel this agreement and/or to claim immediate payment and/or specific performance from the defaulting party whether or not the due date for payment and/or performances has arrived.
- 8.3 The foregoing is without prejudice to such other rights as the aggrieved party may have at law.

9. WARRANTIES AND GUARANTEES

- 9.1. All products quoted on should carry a full original manufacturer's guarantee;
- 9.2. The bidder warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and incorporates all recent improvements in design and materials. The bidder further warrants that all goods supplied under this contract shall have no defect, arising from design, materials, or workmanship (except when the design and/or material are specifically required by the Sedibeng District Municipality's specifications);
- 9.3. The Sedibeng District Municipality shall promptly notify the bidder in writing of any claims arising under warranty of the product. The bidder shall bear the costs of any such claims, unless such claims arise as a result of any negligent act or omission on the part of the Sedibeng District Municipality; and
- 9.4. Upon receipt of such notice, the bidder shall, within five (5) working days after notification, and with all reasonable speed, repair or replace the defective goods or parts thereof, without cost to the Sedibeng District Municipality.

10. DISPUTE RESOLUTION

10.1 Any dispute which may arise out of the operation of this agreement shall be referred to a joint committee comprising of the duly authorised representatives of Sedibeng and the Service Provider, who will use their best endeavours to resolve the dispute within 14 (fourteen) days of it having been referred to them.

10.2 In the event that the dispute fails to be resolved as envisaged in 8.1 above, the matter shall be referred to a mutually acceptable suitably qualified third party for arbitration.

10.3 The arbitration shall be held:

10.3.1 At a mutually agreed venue by the parties;

10.3.2 On the basis that the proper law of the agreement contained in this clause and of the contract in which this clause is contained shall be the law of the Republic of South Africa; and

10.3.3 With only the legal and other representatives of the parties to the dispute present there.

10.4 The Arbitrator shall be, if the matter in dispute is principally:

10.4.1 A legal matter, a practising advocate or attorney of at least 5 (five) years standing;

10.4.2 An accounting matter, a practising chartered accountant of at least 5 (five) years standing; and

10.4.3 Any other matter, an independent person, agreed upon between the parties.

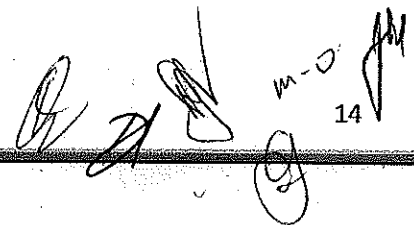
10.5 Should the parties fail to agree on an Arbitrator within 14 (fourteen) days after giving of notice an Arbitrator shall be appointed at the request of either party to the dispute by the President of the Legal Practice Council of the Northern Provinces.

10.6 The Arbitrator shall have the power to fix all procedural rules for the holding of the arbitration, including discretionary powers to make orders as to any matters which he may consider proper in the circumstances of the case with regard to submissions, pleadings, discovery, inspection of documents, examination of witnesses and any other matter relating to the conduct of the arbitration. The Arbitrator may receive and act on all such evidence, whether oral or written, strictly admissible or not, as he in his discretion may deem fit.

10.7 The award of the Arbitrator shall be final and binding upon the parties and may be made an order of any court of competent jurisdiction.

11. FORCE MAJEURE

11.1 Neither party will be liable for any failure to meet any of its obligations in terms of this agreement or any delay in meeting them, to the extent to which the failure or delay is caused by any circumstances whatsoever which are beyond its reasonable control, including but not limited to any labour disputes, strikes or lockout (excluding labour disputes, strikes and lockouts confined mainly to employees of either party), war, riot civil commotion, any order or regulation of any government or other lawful authority meeting the above requirements or any other cause beyond the reasonable control of that party.

 m-o 14

11.2 Any inability to meet a payment due by one party to the other because of lack of funds will in no circumstances be treated as an event of force majeure.

11.3 The affected party must give notice in writing to the other party immediately upon the occurrence of an event of force majeure.

11.4 Should the force majeure prevent performance of a material obligation for a period exceeding 30 (thirty) days, either party may cancel this agreement on written notice to the other, but will not be entitled to recover any damages which it may suffer as a result of such termination.

12. DOMICILIA AND NOTICES

12.1 The parties choose as their *domicilia citandi et executandi* for all purposes arising from or pursuant to this agreement the following addresses:

12.1.1 Sedibeng District Municipality : Civic Centre
Cnr Leslie and Beaconsfield Avenues
Vereeniging
1939

12.1.2 Service Provider : 670 Arthur Street
: Garsfontein
: Pretoria
: 0081

12.2 The parties shall be entitled by way of a written notice to vary their *domicilia* to any other addresses within the Republic of South Africa, which is not a post office box or poste restante

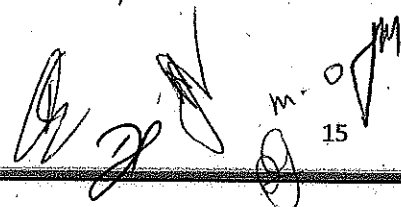
12.3 All notices given in terms of this agreement shall be in writing and any notice given by any party to another which;

12.3.1 Is delivered by hand or transmitted by facsimile shall be deemed to have been received by the addressee on the first business day after the date of delivery or transmission, as the case may be; and

12.3.2 If posted by prepaid registered post from an address within The Republic of South Africa to the addressee at his *domicilium* address for the time being shall be deemed to have been received by the addressee on the 14th (fourteenth) day after the date of such posting.

13. VARIATION

No addition or variation to, consensual cancellation or novation of this agreement and no waiver of any right arising from this agreement or its breach or termination shall be of any force or effect unless reduced to writing and signed by all the parties or their duly authorised representatives.


15

14. RELAXATION

No latitude, extension of time or other indulgence which may be given or allowed by one party to the other in respect of the performance of any obligations hereunder or enforcement of any rights arising from this agreement shall under any circumstances be construed to be an implied consent by such party or operate as a waiver or a novation of, or otherwise affect any of that party's rights in terms of or arising from this agreement or stop such party from enforcing, at any time and without notice, strict and punctual compliance with each and every provision or term hereof.

15. SEVERABILITY

The terms, conditions and undertakings contained in this agreement shall each be construed as an agreement and undertaking independent of any other provisions of this agreement. The parties hereby expressly agree that it is not the intention of any party to violate any public policy, statutory or common law, and that if any sentence, paragraph, clause or combination of the same is violation of the Law of the Republic of South Africa, such sentence, paragraph, clause or combination of the same alone shall be void in the jurisdiction where it is unlawful, and the remainder of such clause in this agreement shall be binding upon the parties hereto. The parties further acknowledge that it is their intention that the provisions of this agreement be binding only to the extent that they may be lawful under existing applicable law of the Republic of South Africa, and in the event that any provision hereof is determined to be overly broad or unenforceable, the parties hereto agree to the modification of such provisions to the minimum extent required to make them valid and enforceable.

16. CESSION AND SUB-CONTRACTING

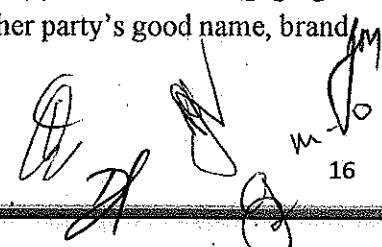
The Service Provider shall not cede, sub-contract, assign, transfer, make over or delegate any right or obligation acquired or incurred in terms of this agreement, without prior written consent of Sedibeng.

17. ASSIGNMENT

Neither party shall be entitled to assign this agreement nor all or any of their rights and obligations hereunder without the prior written consent of the other.

18. CODE OF CONDUCT AND ANTI-CORRUPTION LAWS

- 18.1. The Parties agree to: (i) act at all times in a fair, honest and reputable manner and to ensure that all of its employees also act in such a manner; (ii) use reasonable efforts to promote and market each other's business, at all times consistent with good business practices, legal requirements and ethics, and in a manner that reflects favourably on the goodwill and reputation of each party's business; (iii) avoid deceptive, misleading or unethical practices that are or might be detrimental to itself and the other party; (iv) refrain from making any false or misleading representation with regards to itself or the other party; (v) refrain from engaging in any act or omission that might adversely affect, or damage the other party's good name, brand, goodwill and/or reputation.



16

18.2. Neither party shall engage in any unlawful trade practices or any other practices that are in violation of the Anti-Corruption Laws in connection with any actions or activities associated with this Agreement or in connection with the relationship between the Parties. Each party shall ensure that neither it nor its subcontractors and agents: either directly or indirectly, seek, receive, accept, give, offer, agree or promise to give any money, facilitation payment, or other thing of value from or to anyone (including but not limited to government or corporate officials or agents), as an improper inducement or reward for or otherwise on account of favourable action or forbearance from action or the exercise of influence; or fail to establish appropriate safeguards to protect against such prohibited actions. Each party shall, upon request from the other party, provide evidence of the steps being taken to avoid prohibited actions, including the establishment of policies, practices, and/or business controls with respect to these laws. For the purposes of this clause "Anti-Corruption Laws" shall mean "any applicable foreign or domestic anti-bribery and anticorruption laws and regulations, including but not limited to the Foreign Corrupt Practices Act, 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. (United States of America); Bribery Act, 2010, as amended, c.23, § 1 (United Kingdom); and the Prevention and Combating of Corrupt Activities Act, 2004, as amended (Republic of South Africa), as well as any laws intended to implement the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

19. WHOLE AGREEMENT

This agreement constitutes the whole agreement between the parties as to the subject matter hereof and no other agreement, representations and/or warranties between the parties other than those set out herein shall be binding on the parties.

DATED AND SIGNED AT VEREENIGING ON THIS THE 14 DAY OF May 2025

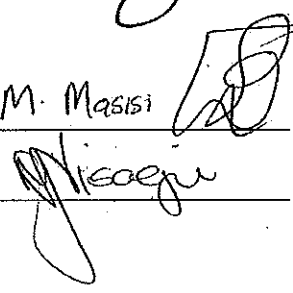

MOTSUMI MATHE

AS WITNESSES:

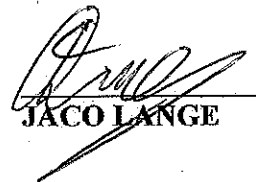
1

M. Masisi

2

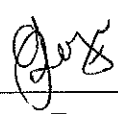


DATED AND SIGNED AT VEREENIGING ON THIS THE 15 DAY OF May 2025


JACO LANGE

AS WITNESSES:

1



2



"ANNEXURE A – PRICING SCHEDULE"



Phone: 012-247-5100

Email: jaco@vpnt.co.za

Web: https://www.vpnt.co.za

Hardware - ONCE OFF

Product Details	Price	Qty	Total Ex VAT
Firewall Hardware	R74 421,00	2	R148 842,00
Dell PowerEdge R250			
- Intel Xeon E-2314 2.8GHz, 8M Cache, 4C/4T, Turbo (65W) 4 x Dell 32GB - 2RX8 DDR4 UDIMM 3200MHz ECC 3 x Dell 960GB SSD SATA Mix Use 6Gbps 512e 2.5in - Broadcom 5720 Dual Port 1Gb On-Board LOM 3 Year Basic Warranty			
High-speed dual-band Wi-Fi router	R3 899,00	1	R3 899,00
Ubiquiti Access Point UniFi AC PRO			
Subtotal:			R152 741,00

Services & Software - MONTHLY

Product Details	Price	Qty	Total Ex VAT
PROVISIONING OF BANDWIDTH (last mile provider)			
Dedicated Fibre 1:1 Contention 100 MBPS	R15 731,00	1	R15 731,00
Please note: This service is on Telkom Last mile. Reason for this is that the existing fibre at Sediberg is from GBN and is on DFA infrastructure. To provide the Council with a truly redundant and high available internet connection we are quoting on a different last mile provider i.e. Telkom			
Management, monitoring and reporting fees	R400,00	1	R400,00
Response time to bandwidth concerns is 2 hours			
ANALYSIS OF INTERNET TRAFFIC			
Proposed proxy traffic analyser	R650,00	1	R650,00
NetFlow collector and analyser	R650,00	1	R650,00
Management, monitoring and reporting fees	R650,00	1	R650,00
Web hosting services			
Website domain hosting and technical support	R1 855,00	1	R1 855,00
Website standard maintenance	R650,00	1	R650,00

18



Phone: 012-247-5100

Email: jaco@vpnt.co.za

Web: <https://www.vpnt.co.za>

Services & Software - MONTHLY

Product Details	Price	Qty	Total Ex VAT
MAIL SCANNING			
Provisioning of mail scanning services (450 users) Perception Point Advanced Email Security SaaS Perception Point's Advanced Email Security Solution is a next-gen email security software that prevents APTs, phishing, malware, ATO, impersonation, and BEC attacks with the speed, scale, and agility of the cloud.	R14 590,00	1	R14 590,00
High availability (HA) cluster	R0,01	1	R0,01
Management, monitoring and reporting fees	R400,00	1	R400,00
Compliance to two (2) hour response time - Yes			
FIREWALL SERVICES			
Firewall software provisioning and support x 2	R1 300,00	1	R1 300,00
High availability (HA) cluster	R300,00	1	R300,00
Firewall standard installation and maintenance	R650,00	1	R650,00
User identity management with LDAP integration	R650,00	1	R650,00
Backup, recovery and reconfigurations	R300,00	1	R300,00
Support, maintenance and reporting	R650,00	1	R650,00
Compliance with provisioning a firewall supporting bandwidth throughput of at least 1 Gb/s - Yes			
Data routing, DHCP and DNS protocols			
Setup, routing, troubleshooting, optimization etc. Includes Auvik Network Management & Monitoring Software for 50 Switches, All Wireless AP's, & Firewall	R12 500,00	1	R12 500,00
Compliance to two (2) hour response time - Yes			
Provisioning and management of VPN			
Services, support and reporting	R650,00	1	R650,00