

**INVITATION TO TENDER FOR INTERNET SERVICE PROVISION**

**Date:** 23<sup>rd</sup> January 2024

**Dateline for Submission:** 7<sup>th</sup> February 2024 by 5PM

**INTERNET SERVICE PROVISION TENDER TECHNICAL SPECIFICATIONS**

***GENERAL:***

1.1 These specifications describe the requirements for each of the item as per required specifications. Bidders are requested to submit with their offers the detailed specifications, brochures, catalogues, etc. for the products they intend to supply for this tender.

1.2 Bidders must indicate on the specifications/requirements sheets whether they comply with each specified requirement for various sites and equipment. All the requirements for connectivity and capacities of the equipment to be supplied shall not be less than those required in these specifications.

**1.3 Backup**

The bidder should propose a secondary backup link which should be from a different switch station to serve as backup at the Country Office of Healthcare Foundation Organization (HFO). A clearly stated technical diagram with an alternative back-up switch should be provided for the backup links. Clearly demonstrate how automatic failover and load balancing will be achieved and the equipment to be used for this purpose.

1.4 A web-based network monitoring tool (s) MUST be provided with a user-friendly GUI with capabilities of bandwidth allocation, network monitoring to the node, remote LAN access (VPN) sessions, content filtering and management of the wireless environment, real time Bandwidth usage monitoring interface. Should have the ability to report any faults giving exact location and identification of the faulty equipment as well as sending notification to the network admin. A smart visual display unit of not less than 46" must be supplied with this solution and be mounted in the monitoring room to display real-time utilization of the bandwidth in the Country Office and easy network monitoring. And in case of any available internet monitoring tools which can be used easily within the mentioned environment should be clearly described by the bidders.



1.5 On security, the connectivity must guard against malicious spam or attacks (e.g. denial of service attacks, computer viruses, spams and Junk mails) to be perpetrated from any network external to Healthcare Foundation Organization Country head office.

1.6 Network should be able to support Voice Service integration (both Fixed and GSM Voice) with installation of at least 4 extensions for communication. The extensions will be provided by Healthcare Foundation Organization in case it is needed.

1.7 There should be service guarantees in terms of availability and reliability through well designed and protected circuits on the core network.

1.8 Service Provider's Primary and Backup links should be backhauled on different networks that are all independently interconnected. This being a managed service, the bidder must demonstrate how they will achieve this independence at the core and access levels for each location, thereby ensuring that HFO will be guaranteed of service even in case of a single circuit failing.

1.9 The service provider MUST provide connectivity to different international internet gateways that should offer HFO high levels of redundancy to the internet with auto fail over mechanisms.

1.10 Specified traffic will be secure (i.e., encrypted by the network using internationally approved encryption techniques and standards), and will be suitable for carrying classified information.

1.11 All the continuously available services shall be scheduled to be available 365 days a year and 24 hours a day, apart from maintenance times which may be scheduled or emergency in nature.

1.12 A separate draft of Service Level Agreement (SLA) should be provided to ensure 99.9% availability guarantee of the services.

1.13 Dedicated Public IP addresses for particular field sites to enable remote administration of routers and the entire network from HFO Head Office or suitable Network Address Translation to enable access of shared resources should be provided.

#### 1.1.0. Bandwidth Requirements:

Bandwidth Requirement for Juba Office and Field Sites in Mbps respectively.

S/N	Location	Band Width	Connectivity / Media
1	HFO Country Head Office Juba	15Mbps  15MBPS	Fibre  WIMAX
2	New Fangak	3mbps	VSAT
3	Diel / Canal Pigi	3mbps	VSAT
4	Manajang	3mbps	VSAT
5	Keew	3mbps	VSAT
6	Leer	3mbps	VSAT



## 2.0. SUPPORT AND MAINTENANCE

### 2.1. Preventive Maintenance:

The successful bidder will be responsible for: -

1. Repair and replacement of faulty network communication components for all the active WAN devices for a given warranty periods.
2. Provision of continuous second and third level technical support that will minimize unplanned downtime in order to avoid disruption of service delivery for HFO LAN and WAN infrastructure and components for a given period of time by HFO.
3. Provision of quarterly preventive maintenance for the given period under warranty.
4. Conducting network vulnerability testing using qualified staff/experts once a year.
5. Coordinating with HFO I.T focal Person for network related changes/updates, etc.
6. Reporting Network hardware/software related problems to HFO I.T Focal person.

## 3.0. COMPLIANCE TO TECHNICAL SPECIFICATIONS EVALUATION CRITERIA.

Response to compliance to all Technical Specifications is **MANDATORY**. Bidders **MUST** respond to **ALL** the technical requirements on a clause by clause basis stating clearly how their solution meets the requirements. Responses to compliance to technical specifications in any other way other than clause by clause will be treated as NON-RESPONSIVE.

The Technical requirements are as follows: These are mandatory technical requirements and bidders **MUST** respond to each of them clause by clause (**No's 1 – 10**) in writing clearly indicating how they will achieve/meet each requirement. Responses to compliance to technical specifications in any other way other than clause by clause will be treated as **NON-RESPONSIVE**

	<b>Minimum specifications for links 1&amp;2</b>	Bidders response (YES/NO)
1	The back-bone for the secondary links should not use the same backbone of the main link.	
2	The provider must demonstrate the ability to offer 24/7/365 Online & Onsite Support for each site	
3	The provider must be able to provide Public IP Addresses for each link – bidder must provide proof of ownership. The provider should capture the AS details indicating the public IP ownership and peering details	
4	Provision of automatic failover/load balancing between the main link and the Back-up links with real time monitoring.	
5	Network provider must be able to integrate security features – bidder must provide details.	



6	Any other details as may be required for continuity and best performance of these Links.	
7	The service provider needs to provide daily, weekly and monthly link availability and utilization reports with a portal for access of the graphs. Refer to requirements for network monitor	
8	<p>The network should be able to support MPLS or SD-WAN – Bidder must provide supporting evidence to include; Traffic Engineering: Set path that the traffic will have to take through the network.</p> <ul style="list-style-type: none"> <li>❖ More specifically, each class of traffic, data, voice and video will be set for individual performance characteristics.</li> <li>❖ Quality of Service: Support for network convergence to allow introduction of new services like voice and video.</li> <li>❖ Network Redundancy: Rerouting traffic through the next optimum path with a failover time of 50ms or less.</li> <li>❖ Protocol Independent forwarding.</li> </ul>	
9	Due to the dynamic nature of HFO operations, the bidder should accept this to be a flexible contract where links especially to HFO Field offices can be added, relocated or removed within the contract period and the billing adjusted accordingly without contract amendments. Bidders should provide costs of relocation, removal or new installation in the pricing.	
10	Each link <b>must</b> have 99.9% uptime with proof of measurement tools.	

#### 4.0. WIFI NETWORK SPECIFICATIONS EVALUATION CRITERIA.

The Wi-Fi network shall be based on the following technical specifications. Bidders are expected to respond on a clause by clause basis stating clearly how their solution meets the requirements. These are **mandatory technical requirements** and bidders **MUST** respond to each of them clause by clause (**All items**) in writing clearly indicating how their solution meets the requirements. Responses to compliance to Wi-Fi network technical specifications in any other way other than clause by clause will be treated as **NON-RESPONSIVE**:

Items	Requirements	Bidder's Response
Coverage	Deploy a Wi-Fi Network that provides sufficient coverage of the Field Office. The bidders' proposal should be guided by the site visit findings. Sufficient coverage is described as being able to provide at least downlink signal strength of 75dB and 38dB uplink. Concurrent Clients 200+	



Authentication	The Wi-Fi network should have a secured captive portal for authentication.	
Management	Fully managed network service. Operator responsible for maintaining uptime of greater than 99% Support line for the service <ul style="list-style-type: none"> <li>• Remote configuration and management through Web browser, SNMP or telnet with Command Line Interface (CLI)</li> <li>• SNMP management supports SNMP MIB I, MIB II,</li> <li>• 802.11 MIB and proprietary configuration MIB</li> <li>• POE 48V</li> </ul>	
Technology	802.11g/n network with 2.4ghz access Antennas 2.4Ghz, 5Ghz	
Wireless Security	WEP, WPA-PSK, WPA Enterprise(WPA/WPA2, TKIP/AES)	

#### 4.1. Wireless Access Point per Location:

Below are the number of access points at HFO Country Head Office and Field Sites.

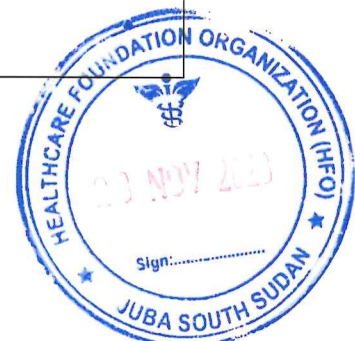
FIELD SITES	NUMBER OF Aps
Juba	2
New Fangak	1
Diel/ Canal Pigi	1
Manajang	1
Keew	1
Leer	1



**4.2. NETWORK AND E-MAIL SECURITY SPECIFICATIONS EVALUATION CRITERIA.**

The network and E-mail security shall be based on the following technical specifications. Bidders are expected to respond on a clause by clause basis stating clearly how their solution meets the requirements. These are mandatory technical requirements and bidders **MUST** respond to each of them clause by clause (All items) in writing clearly indicating how their solution meets the requirements. Responses to compliance to technical specifications in any other way other than clause by clause will be treated as **NON- RESPONSIVE**.

Items	Requirements	Bidders' Responses
Network E-mail Security	<p>The service should have the Ability to inspect all incoming and outgoing emails to and from the HFO email server (Real-time protection against malware, Worms, DDoS etc.) and block any such emails.</p> <ul style="list-style-type: none"> <li>• Protect against newly observed domain names used as part of an attack.</li> <li>• Protect against display name spoofing and reply-to address mismatches.</li> <li>• Have a complete administrative control and re reply-to address.</li> </ul>	
Awareness and Management	<p>Application Awareness: The service must be able to identify, allow, block or limit applications regardless of port, protocol etc. This should provide visibility into unknown &amp; proprietary application within the organization network.</p> <ul style="list-style-type: none"> <li>• Identity Awareness: The solution should Identity awareness for granular control of applications by specific users, group of users and machines that the users are using.</li> <li>• Centralized Management, Administration, Logging and Reporting: Separate management solution should be available for management, logging and reporting. This helps organizations in log analysis and policy management. Central management should also give you the ability to automate routine tasks, reuse elements and employ shortcuts and drill-downs to produce</li> </ul>	



	<p>maximum efficiency with minimal effort.</p> <ul style="list-style-type: none"> <li>• Deep Packet Inspection: The capability should ensure the various pieces of each packet are thoroughly examined to identify malformed packets, errors, known attacks and any other anomalies. DPI can rapidly identify and then block Trojans, viruses, spam, intrusion attempts and any other violations of normal protocol communications.</li> <li>• Integrated IPS: The IPS functionality should be present on the solution</li> <li>• Scan for viruses and malware in allowed applications</li> <li>• Remote Access VPN</li> <li>• The service should provide users with secure, seamless access to corporate networks and resources when traveling or working remotely. Privacy and integrity of sensitive information is ensured through multi-factor authentication, endpoint system compliance scanning and encryption of all transmitted data.</li> </ul>	
--	--	--

#### 5.0. Mandatory Evaluation Criteria (MEC).

NO	Requirements	Indicate pages submitted in the Tender
<b>MEC 1</b>	Submit 1 (one) Original and 1 (one) copy of the tender document	
<b>MEC 2</b>	Bidding documents must be paginated. All bidders are required to submit their documents paginated in a continuous ascending order from the first page to the last in this format; (i.e. 1,2,3..n)where n is the last page	
<b>MEC 3</b>	Submit a copy of company's Certificate of Registration Incorporation/Business name	
<b>MEC 4</b>	Provide copy of the company's current SSRA (South Sudan Revenue Authority) Tax Compliance Certificate	
<b>MEC 5</b>	Submit valid Government Business Permit.	
<b>MEC 6</b>	Duly completed Tender form signed and Stamped.	



<b>MEC 7</b>	Provide proof of authorization & Support by the equipment manufacturers to sell/service the product.	
<b>MEC 8</b>	Provide Internet Service Provider License by the National Communications Authority of the Republic of South Sudan.	
<b>MEC 9</b>	Submit with tender a certificate of registration with the ICT Authority of South Sudan.	
<b>MEC 10</b>	Provide a warranty and free maintenance for a period of 12 months for any new equipment bought for the installation.	
<b>MEC 11</b>	Tenders submitted by a joint venture of two or more firms as partners or using a designated sub-contractor shall provide a copy of agreement/contract and comply with HFO Terms of requirements: -	

**Interested Internet service providers should submit their details to [logp.healthcarefoundation.org@gmail.com](mailto:logp.healthcarefoundation.org@gmail.com) / [log@hfo-ss.org](mailto:log@hfo-ss.org) copy to [isprocurement@hfo-ss.org](mailto:isprocurement@hfo-ss.org) Or Hard Copy can be Submitted to Logistic Department in a sealed envelope to HFO Juba Office Located at Behind Catholic University of South Sudan /Plot No: 143 blocks Juba Nabari, Tongpiny**

**NB:** HFO has an installed internet system running currently in Juba Office and most of its Field Sites with MiKroTik, iDirect Modem: Model: X1 in place. Any point of changes and demands for new internet appliances and recommendations can be determine through consultation with the I.T Focal Person. And any recommendation on changes of the previous systems and additional requirements of internet hardware and software or upgrade in the system needed, should clearly be noted by the clients in their bidding documents and cost should be indicated in the total amount of the service.

And all routers in different field sites Must be accessible by the I.T Focal Person in the Country Head Office.

