Network Infrastructure Upgrade
Request for Proposal

March 25, 2024

I. INTRODUCTION

Médecins Sans Frontières/Doctors Without Borders Eastern Africa (MSF EA) –is soliciting proposals from vendors that are qualified to provide Network Infrastructure Upgrade services.

Proposals are due by 5:00 pm, ET, on 8th April 2024. Vendors are expected to prepare their proposal using this RFP as a template.

II. OVERVIEW OF MÉDECINS SANS FRONTIÈRES

A. The Organization

A group of French doctors and journalists in the late 1960s were responding to the humanitarian crisis in Biafra, Nigeria as part of the International Red Cross. Protesting the protocols governing Red Cross workers at the time, which forbid them from speaking out about what they were seeing on the ground, led them to form their own medical humanitarian organization – with a mandate not only to provide emergency medical care, but also to 'bear witness' on behalf of their patients. This new brand of humanitarianism would reinvent the concept of emergency aid. They were to become Médecins Sans Frontières (MSF), known internationally in English as Doctors Without Borders.

B. MSF Eastern Africa

MSF Eastern Africa is the regional institutional office for Médecins Sans Frontières/Doctors Without Borders (MSF) in East Africa, based in Nairobi, Kenya. The office focuses on representation and networking, including with humanitarian organizations and authorities, recruiting and supporting staff from the region, communications and fundraising, as well as on other dossiers of importance to MSF.

III. NETWORK INFRASTRUCTURE UPGRADE PROJECT DETAILS

A. Background

Despite the transition from a Branch office to a Partner Section and the subsequent increase in operational support and hosting capacity, MSF Eastern Africa's core IT infrastructure has remained unchanged for over four years. A recent assessment highlighted the imperative need for improvements to sustain operational efficiency, facilitate future growth, and fortify our security posture.
Objectives of this improvement/upgrade initiative:

1. Supporting scalability, organizational growth and operational expansion (new Operational Directorate).
2. Replace/dispose obsolete equipment.
3. Improve security by design.
4. Optimize network resources for maximum gain/benefit.
5. Enhance business continuity.

Following your participation in the initial request for information, you are hereby invited to submit a precise proposal for the scope below.

B. Overview of Current Infrastructure

Item	Units	Description
Floor Plan	3	All floors have 2 wings each (A & B) except one. So in total there are 5 wings.
Network Switches		Ubiquity Edge Switch 8 port Installed as Core Switch. Status: EoL - Undefined
		Ubiquity Unifi Switch 24 Port (250W) Installed per floor for users. Status: EoL - Undefined
Access Points	15	Ubiquity (UAP-AC-LR) Working perfectly 3 units per floor distribution
Firewall	2	Palo Alto (PA 220) Physical appliance with redundancy.
Routers	4	Cisco 4200 Series Huawei (AR 160) Cisco 1900 Series Cisco 1800 Series Supporting Internet Links
Internet Links	2	Working perfectly Bandwidth: 100Mbps from each link Need to improve load balancing to utilize the redundant link more.
Network Design		Flat network
Power Backup		Various UPS's Not sufficiently supporting all critical electrical installations – i.e 17 meeting rooms, 6 printers, 5 other rooms. Need overhaul
No. of Users	160	60% daily occupancy. Rest working remotely. 40% growth projection over the next 2 years.
Servers	2	HPE ProLiant DL380 G7 Not virtualized
CCTV Cameras	22	Dahua Technology; 1 NVR

C. Scope of Work Overview

Supply of equipment	• Firewalls • Switch • Network monitoring tools • Access points • CCTV Backup appliance • Power inverter backup
Network	• Redesign of the Local Area Network putting emphasis on security enhancements and improved services • Configuration of Network firewall in high availability mode • Network firewalls operate as a combination of user and edge firewall roles. • Installation and configuration of Network and server management and monitoring tools. • Configuration of Network switches • Installation of Configuration of Wi-Fi network • Cabling cleanup and cable management for Data Centre and user areas • VPN setup and authentication to Azure.
Servers	• Installation of virtualization hypervisor on the provided server hardware • Provisioning of virtual machines on the server hardware • Installation and configuration of active directory server (VM) hosted on Microsoft Azure • Integration of the active directory server with Office 365 tenant. • Installation and configuration of on-premises backup Active Directory server.
Backup	• Setup Network based backup solution. • Installation of backup software • Setup backup schedules for CCTV footage • Setup of power inverter backup to replace UPS backups.
Service Level Agreement	Annual SLA for the entire network infrastructure.

D. Detailed Scope/Project Requirements

a. Supply of equipment & Licenses

Firewall

		QTY
FIREWALL	**SPECS**	**2**
VENDOR	**FORTINET**	

SUBSCRIPTION	FORTIGUARD ENTERPRISE PROTECTION (1 YR AND 3 YRS) OPTIONS	
Hardware Accelerated GE RJ45 Ports	12	
Hardware Accelerated GE RJ45 Management	1	
Hardware Accelerated GE RJ45 HA	2	
Hardware Accelerated GE RJ45 DMZ Ports	1	
Hardware Accelerated GE SFP Slots	4	
GE RJ45 WAN Ports	2	
IPS Throughput 2	2.6 Gbps	
NGFW Throughput 2	1.6 Gbps	
Threat Protection Throughput	1 Gbps	
Firewall Throughput (Packet per Second)	15 Mbps	
Onboard storage	480Gb SSD	
Concurrent Sessions (TCP)	1.5 MILLION	
New Sessions/Second (TCP)	56000	
SSL-VPN Throughput	1 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
High Availability Configurations	YES	

Switch – (Ruijie)

		QTY
NETWORK SWITCH	**Ruijie**	**1**
COMPATIBLE 1G MULTIMODE SFP		**5**
1 YEAR SUPPORT		**1**
SPECIFICATIONS		
SWITCH	48 x 10/100/1000M adaptive electrical ports, 4 x 1G/10G SFP+ ports, supporting PoE remote power supply and the maximum PoE output power of 1480 W	
RG-PA1000I-P-F	1000 W AC power module, PoE power module	
DUAL POWER CONFIGURATION	YES	
Packet forwarding rate	132 Mpps	
Switching capacity	176 Gbps	
MAC address table size	32,000	

ARP table size	4,000	
Number of IPv4 unicast routes	8,000	
Number of IPv4 multicast routes	2,500	
Number of IPv6 unicast routes	4,000	
Number of IPv6 multicast routes	1,200	
Number of ACEs	Ingress: 3,500	
	Egress:1,500	
Number of VSU members	4	
VLAN translation	4,094	
switching	Jumbo frame (maximum length: 9216 bytes)	
	IEEE 802.1Q (4K VLANs)	
	Voice VLAN	
	Super VLAN and private VLAN	
	MAC VLAN, port-based VLAN, protocol-based VLAN, and IP-subnet based VLAN	
	GVRP	
	Basic QinQ	
	Selective QinQ	
	STP, RSTP, and MSTP	
	ERPS (G.8032)	
	LLDP/LLDP-MED	
	LACP (IEEE 802.3ad)	
IP service	ARP	
	DHCP client, DHCP relay, and DHCP server	
	DHCP snooping	
	DNS	
	DHCPv6 client and DHCPv6 relay	
	DHCPv6 snooping	
	Neighbor Discovery (ND) and ND snooping	
IP routing	Static routing	
	RIP, RIPng	
	OSPFv2, OSPFv3, IS-ISv4, ISv4, and IS-ISv6	
	BGP4 and BGP4+	

	IPv4 and IPv6 VRF	
	IPv4 and IPv6 PBR	
Multicast	IGMP v1/v2/v3, and IGMP proxy	
	IGMP v1/v2/v3 snooping	
	PIM-DM, PIM-SM, and PIM-SSM	
	MSDP	
	MLD v1/v2	
	MLD snooping v1/v2	
	PIM-SMv6, PIM-SSM v6	
ACL and QoS	Standard IP ACLs	
	Extended IP ACLs	
	Extended MAC ACLs	
	ACL80	
	IPv6 ACL	
	ACL redirection	
	Port traffic identification	
	Port traffic rate limiting	
	802.1p/DSCP/ToS traffic classification	
	Eight priority queues per interface	
	Traffic policing: CAR	
	Congestion management: RR, SP, WRR, DRR, WFQ, SP+WRR, SP+DRR, and SP+WFQ	
	Congestion avoidance: tail drop, RED, and WRED	
	Rate limiting in each queue	
Security	Multiple AAA modes	
	RADIUS and TACAS+	
	Port-based and MAC-based 802.1x authentication	
	Web authentication	
	Allowlist	
	HTTPS	
	SSHv1, SSHv2	

	Global IP-MAC binding	
	ICMP	
	Port isolation and port security	
	IP Source Guard	
	SAVI	
	Gateway ARP anti-spoofing	
	CPP(CPU Protection Policy)	
	NFPP(Network Foundation Protection Policy)	
	Strict and loose RPF	
	uRPF ignoring default routes	
Reliability	REUP, RLDP, DLDP	
	IPv4 VRRP v2/v3 and IPv6 VRRP	
	BFD	
	Link tracing, fault notification, and remote loopback based on 802.3ah (EFM)	
	Hot swapping of power modules and cables	
	3-level fan speed adjustment	
	Fan fault alarm	
Device virtualization	Virtual Switching Unit (VSU)	
NMS and maintenance	SPAN, RSPAN, and ERSPAN	
	sFlow	
	NTP and SNTP	
	FTP and TFTP	
	SNMP v1/v2/v3	
	RMON (1, 2, 3, 9)	
	NETCONF	
	CWMP (TR-069) standard protocol	
	gRPC	
	Cloud and SON	
PoE	IEEE 802.3af and 802.3at	
	Uninterruptible power supply upon hot start	
	Port priority	

CCTV Backup Appliance – Synology

	ON PREMISE BACKUP SOLUTION FOR CCTV	**Synology**	
Hardware Specs			QTY
CPU	CPU Model	AMD Ryzen V1780B	
	CPU Quantity		1
	CPU Architecture	64-bit	
	CPU Frequency	4-core 3.35 (base) / 3.6 (turbo) GHz	
	Hardware Encryption Engine (AES-NI)		
Memory	System Memory	8 GB DDR4 ECC SODIMM	
	Memory Module Pre-installed	8 GB (8 GB x 1)	1
	Total Memory Slots		2
	Maximum Memory Capacity	32 GB (16 GB x 2)	
Storage	Drive Bays		8
	Maximum Drive Bays with Expansion Unit	18 (DX517 x 2)	
	M.2 Drive Slots	2 (NVMe)	
	Hot Swappable Drive*		
	Compatible HDD Drives - SATA	8TB	6
	RAID CONFIGURATION	RAID 5 /RAID 6	
External Ports	RJ-45 1GbE LAN Port	2 (with Link Aggregation / Failover support)	
	RJ-45 10GbE LAN Port		1
	Out-of-Band Management LAN Port		1
	USB 3.2 Gen 1 Port*		3
	eSATA Port		2
PCIe	PCIe Expansion	1 x Gen3 x8 slot (x4 link)	
Appearance	Size (Height x Width x Depth)	166 mm x 343 mm x 243 mm	
	Weight	6.2 kg	
Others	System Fan	120 mm x 120 mm x 2 pcs	
	Fan Speed Mode	Full-Speed Mode	

		Cool Mode	
		Quiet Mode	
	Easy Replacement System Fan		
	Brightness Adjustable Front LED Indicators		
	Power Recovery		
	Noise Level*	23.6 dB(A)	
	Scheduled Power On / Off		
	Wake on LAN / WAN		
	Power Supply Unit / Adapter	250 W	
	AC Input Power Voltage	100V to 240V AC	
	Power Frequency	50/60 Hz, Single Phase	
	Power Consumption	87.93 W (Access)	
		28.37 W (HDD Hibernation)	
	British Thermal Unit	300.23 BTU/hr (Access)	
		96.87 BTU/hr (HDD Hibernation)	
Temperature	Operating Temperature	0°C to 40°C (32°F to 104°F)	
	Storage Temperature	-20°C to 60°C (-5°F to 140°F)	
	Relative Humidity	5% to 95% RH	
Certification	FCC		
	CE		
	BSMI		
	VCCI		
	RCM		
	EAC		
	CCC		
	KC		

Access Points – 15

MANAGEMENT	Lifetime Free Cloud Management subscription	
Radio design	Dual radio	
	Radio 1: 2.4 GHz, two spatial streams, 2x2 MU-MIMO	

	Radio 2: 5 GHz, two spatial streams, 2x2 MU-MIMO	
Operating frequencies	Radio 1, 802.11b/g/n/ax:	
	● 2.400 GHz to 2.4835 GHz, ISM	
	Radio 2, 802.11a/n/ac/ax:	
	● 5.150 GHz to 5.250 GHz, U-NII-1	
	● 5.250 GHz to 5.350 GHz, U-NII-2A	
	● 5.470 GHz to 5.725 GHz, U-NII-2C	
	● 5.725 GHz to 5.850 GHz, U-NII-3/ISM	
	Note: Country-specific restrictions apply.	
Data rates	Combined peak data rate: 1.775 Gbps	
	2.4 GHz radio, 574 Mbps	
	● Two spatial stream Single User (SU) MIMO for up to 574 Mbps wireless data rate to individual 2SS HE40 802.11ax client devices (max.)	
	● Two spatial stream Single User (SU) MIMO for up to 287 Mbps wireless data rate to individual 2SS HE20 802.11ax client devices (typical)	
	5 GHz radio, 1.2Gbps	
	● Two spatial stream Single User (SU) MIMO for up to 1.2 Gbps wireless data rate to 2SS HE80 802.11ax client devices (typical)	
Data rate set	The following 802.11-compliant data rates in Mbps are supported:	
	2.4 GHz radio	
	● 802.11b: 1, 2, 5.5, 11	
	● 802.11g: 1, 2, 5.5, 6, 9, 11, 12, 18, 24 ,36, 48, 54	
	● 802.11n: 6.5 to 300 (MCS0 to MCS15, HT20 to HT40)	
	● 802.11ax: 8.6 to 574 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE40)	
	5 GHz radio	
	● 802.11a: 6, 9, 12, 18, 24, 36, 48, 54	
	● 802.11n: 6.5 to 300 (MCS0 to MCS15, HT20 to HT40)	
	● 802.11ac: 6.5 to 867 (MCS0 to MCS9, NSS = 1 to 4, VHT20 to VHT80)	

	• 802.11ax: 8.6 to 1,200 (MCS0 to MCS11, NSS = 1 to 2, HE20 to HE80)	
Packet aggregation	802.11n/ac/ax: A-MPDU and A-MSDU	
Antenna type	Built-in omnidirectional antennas (two 2.4 GHz antennas and two 5 GHz antennas)	
Max. antenna gain	2.8 dBi in 2.4 GHz and 3.6 dBi in 5 GHz	
	The downtilt angle for the maximum gain is roughly 30 degrees.	
	With reference to the pattern of each antenna of the MIMO radios, the maximum gain of the effective per-antenna pattern is 2.3 dBi in 2.4 GHz and 2.7 dBi in 5 GHz.	
Max. transmit power	2.4 GHz radio: 26 dBm (23 dBm per chain)	
	5 GHz radio: 26 dBm (23 dBm per chain)	
	Note: The transmit power is limited by local regulatory requirements.	
Power increment	Configurable based on requirement	
Radio technologies	802.11b: Direct-Sequence Spread-Spectrum (DSSS)	
	802.11a/g/n/ac: Orthogonal Frequency-Division Multiplexing (OFDM)	
	802.11ax: Orthogonal Frequency Division Multiple Access (OFDMA)	
Modulation types	802.11b: BPSK, QPSK, CCK	
	802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM	
	802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM	
	802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM	
Bluetooth	Bluetooth 5.1	
Antenna type	1 x onboard built-in omnidirectional antenna	
Max. antenna gain	2.4 dBi, with a downtilt angle of roughly 30 degrees	
Max. transmit power	17 dBm (GFSK)	
	14 dBm (π/4-DQPSK, 8-DPSK)	
Receive sensitivity	–95.5 dBm (DH5)	
	–95 dBm (π/4-DQPSK)	
	–87.5 dBm (8-DPSK)	

Fixed service port	Uplink: 1 x 10/100/1000Base-T RJ45 Ethernet port with auto-negotiation	
	● Compliance with IEEE 802.3af standard (PoE)	
	● Auto MDI/MDIX crossover	
	● PoE-PD: 54 V DC (nominal) 802.3af/at/bt (Class 3 or higher)	
	● 802.3az EEE	
Fixed management Port	1 x RJ45 console port (serial console port)	
Status LED	1 x multi-color system status LED	
Button	1 x Reset button	
	● Press the button for shorter than 2 seconds. Then the device restarts.	
	● Press the button for longer than 5 seconds. Then the device restores to factory settings.	
Max. number of BSSIDs	32 (up to 16 BSSIDs per radio)	
STA management	SSID hiding	
	Band steering	
	Each SSID can be configured with the authentication mode, encryption mechanism, and VLAN attributes independently.	
	Remote intelligent perception technology (RIPT)	
	Intelligent client identification technology	
	Intelligent load balancing based on the STA quantity or traffic	
STA limiting	SSID-based STA limiting	
	Radio-based STA limiting	
Bandwidth limiting	STA/SSID/AP-based rate limiting	
Wireless roaming	Layer 2 and Layer 3 roaming	
Authentication and encryption	Remote Authentication Dial-In User Service (RADIUS)	
	PSK, PPSK, web, 802.1X, MSCHAPv2, PEAP, WPA, WPA2, and WPA3 authentication	
	Data encryption: WEP (64/128-bit), WPA-TKIP, WPA-PSK, WPA2-AES, WPA3	

Data frame filtering	Allowlist, static blocklist, and dynamic blocklist	
WIDS	WIDS (Wireless Intrusion Detection System)	
	User isolation	
	Rogue AP detection and containment	
ACL	Dynamic ACL assignment	
	● ACL assignment based on time spans	
	● ACL assignment (complete entry) based on MAC addresses	
	● Execution of pre-configured ACLs (entry index) based on MAC addresses	
CPP	Supported	
NFPP	Supported	
IP service	Static IPv4 address and DHCP-assigned IPv4 address	
	DHCP Snooping, Option 82, DHCP Server, DHCP Client	
Multicast	Multicast-to-unicast conversion	
IPv6 basics	IPv6 addressing, Neighbor Discovery (ND), ICMPv6, IPv6 Ping	
	IPv6 DHCP Client	
IP routing	IPv4/IPv6 static routing	
VPN	PPPoE Client	
	IPsec VPN, up to five IPsec tunnels	
Network management	SNMP v1/v2c/v3	
	Syslog	
	Debugging	
Network management platform	Web-based management (Eweb)	
	Cloud	
User access management	Console, SSH, and Telnet-based management	
	FTP Client and TFTP Client	
Fat/Fit/Cloud mode switchover	When the AP works in Fit mode, it can be switched to Fat mode through an AC.	
	When the AP works in Fat mode, it can be switched to Fit mode through the console port or Telnet.	

Network Monitoring Tools

Widget-based multi-page dashboards	COMPLIED
Easy drag and drop widget placement	
Configure automatic dashboard refresh intervals	
Ability to clone an existing dashboard	
Private and public dashboards	
Flexible graphs capable of displaying regular and aggregate data	
Create map hierarchy trees and use them to navigate through your infrastructure	
Execute a script directly from a dashboard and remediate an issue or display additional information	
Proposed system installation should be supported as a virtual appliance.	
Out of the box monitoring for leading software and hardware vendors:	
Cisco	
HPE	
Microsoft	
IBM	
VMware	
Meraki	
Juniper	
F5	
And many more	
Collect and display inventory information	
Automatically collect and store inventory information:	
Use collected metrics to provide inventory information about your hosts	
Get an overview of your overall inventory by grouping your hosts based on inventory information	
Provide and keep track of geo-map monitoring target coordinates	
Dynamically update existing inventory information from collected metrics	
SLA Monitoring	
Define services and service components with custom SLA calculation logic:	
Analyze status of related services to perform SLA calculation	
Decrease SLA when either single or all of the components of a service are in a problem state	
Create service trees for complex SLA calculations of individual services	

Access daily/weekly/monthly/yearly overviews of your service SLAs	

b. Structured Cabling Enhancement

- Rearrangement and Port Identification: A meticulous rearrangement of ports will be conducted to optimize connectivity. Each port will be systematically identified to facilitate ease of management and troubleshooting.
- Mapping and Labeling: Every critical port will be meticulously mapped and labeled on various patch panels, streamlining identification, and reducing downtime during maintenance.
- Network Topology Redesign: The existing network topology will be redesigned to align with industry standard star topology requirements. This enhancement ensures an efficient and resilient network architecture.
- Cable management from the server room all the way to 150 workstations. Use cable ties such as the one below to ensure neat workstations and cabinets.

Adherence to the following guidelines is also expected:

TASK	REMARKS
Planning	Proper planning is required to coordinate the process professionally, including service downtime during the process.
Cable Routes Determination	Determine if they enter from the top or bottom of the server rack. Then plan the routes to separate power and data cables, and copper data cables and fiber.
Cable Identity	Use of colored cables as well as cable labels to ensure easier cable identification will be employed.
Route and Retain Cables	Cables will be protected at points where they might encounter sharp edges or heated areas. Cable ties and cable managers will be used to this end.
Cable Security	Cables and connectors should be secured to prevent excessive movement and to provide strain relief of critical points.
Thermal issues.	Ensuring the airflow path is rather important, since restrained airflow can cause temperatures rise that would shorten devices' expected lifespan.

c. **Network Segmentation -** The current network structure in the organization, operating on a flat design, faces several challenges, especially in supporting 160+ users spread across three floors. Here are the identified challenges and required fixes through network segmentation:

Challenge	Required Fix
Large subnet	Implement network segmentation by dividing the network into smaller subnets. This will optimize the broadcast domain size, reducing congestion and enhancing overall network efficiency.
DHCP Management issues	Segment the network to create smaller, dedicated subnets, each with its DHCP scope. This approach simplifies DHCP management, mitigates the risk of address exhaustion, and streamlines configuration.
Security concerns in a single flat network	Implement network segmentation to create isolated segments. This establishes barriers between different user groups or functional areas, limiting the impact of security breaches and facilitating more granular control and monitoring.

d. **Server Virtualization and Optimization -** The virtualization process will focus on one of the HPE ProLiant DL380 G7 server units, leveraging HyperV technology. This server will be purposefully repurposed to serve as the host for a suite of access and monitoring tools.

e. **Virtual Server Configuration**

- AD setup on Azure VM as the primary AD with a link to the MSF global tenant. Configure VPN to authenticate from Azure.

- Redundant read-only Active Directory: Ensuring system continuity, a redundant Active Directory will be established as a failover in case of any discrepancies with the Microsoft Azure-hosted Active Directory. All the Windows based licenses will be provided by MSF.
- Bandwidth Management and Network Monitoring Tools: Dedicated virtual servers will be deployed to host essential tools for efficient bandwidth management and network monitoring.

f. Security Measures - integration of robust security measures at every layer, safeguarding the infrastructure against potential threats and vulnerabilities.

g. **Power Inverter setup for power backup -** Inverter Power Backup solution to provide uninterrupted power supply across the entire organization through clean power. This shall supplement the Kenya Power Grid supply for an estimated 4 – 8 hr runtime. Below inverter components are required:

NO	DESCRIPTION	QTY
1	200 AH, 12 Volts gel Batteries	4
2	Original Must 5KVA Inverter/Charger low frequency	1
3	Battery Cabinet with wheels	1
4	Double pole MCB Breaker Complete with housing	1
5	Manual Changeover switch	1
6	Battery fuse rated 200 Amps complete with Handle & housing	2
7	Inverter output power distribution board with 3x 32 Amps MCBs	1
8	AVS 30 Amps switching 70 Amps contactor complete with housing	1
9	Cable lugs pure copper 90 mm	30
10	Battery Cable 90 mm	10
11	Industrial sockets to power UPS	3
12	Red, Black and Green Cables to connect power backup to load	1
13	10mm sq Red, Black, and green cables for inverter incoming power	1

A connected load of 250 watts, for instance, requires less than 270 watts to be supplied by batteries. In addition, the current usable UPS units shall be used to complement the inverter setup and improve on the power reliability in case of any failures and ensure minimal to no interruption.

h. Service Level Agreement for 1 year.
For L2 support on all IT infrastructure issues at MSF.

E. Project Deliverables

a. Supply of equipment in compliance with the specifications provided.
b. Updated network architecture/design.
c. Technical documentation.
d. Training for IT with documented SOPs.
e. Completion report.

IV. INSTRUCTIONS FOR PROPOSAL SUBMISSION

A. Primary Project Contacts

The individual listed below represents the vendors' primary project contact at MSF Eastern Africa. Under no circumstances should vendors contact individual staff at MSF Eastern Africa to discuss any aspect of this Request for Proposal ("RFP") unless directed to by the primary contact. If you have existing business with MSF Eastern Africa, please do not discuss this RFP during those business communications.

For all correspondence regarding this RFP, kindly contact:

procurement@nairobi.msf.org

B. Non-disclosure Agreement

As part of our vendor risk assessment procedures, the successful vendor must complete a non-disclosure agreement prior to signing a contract with MSF Eastern Africa. The MSF Eastern Africa NDA template will be provided.

C. Submission of Questions

If, after reviewing this RFP, you have questions that need to be answered for you to develop a thorough proposal, please email your questions **before 5:00 pm ET on 1st April 2024** to the primary contact listed above in Section IV-A. On **3rd April 2024** MSF Eastern Africa will provide responses to all submitted questions in writing to all RFP recipients.

D. In-Person Meetings with Vendors

Once vendors have responded to the RFP, MSF Eastern Africa will review all responses and determine a short list of vendors who have demonstrated their capacity to meet our needs to move forward in the

RFP process. Vendors will be contacted via email to be notified of their status. Vendors that move forward will then be asked to participate in virtual meetings with MSF Eastern Africa stakeholders. These meetings will last between 1-2 hours.

These meetings are meant to provide the vendors with additional exposure to MSF Eastern Africa stakeholders, allow stakeholders to understand the culture and management of prospective vendors and management, and allow for additional clarification of RFP responses and contract / pricing terms. An agenda will be provided prior to these meetings so vendors will know what topics will be discussed and the time allowed for each topic. A presentation by the vendor about their business and prospective business with MSF Eastern Africa will be included in the agenda. Vendors may also recommend topics for these meetings.

MSF Eastern Africa reserves the right to eliminate vendors from the selection process following these meetings.

E. Proposal Response

Proposals are due by 5:00 pm, ET, on 8th April 2024 You must submit an electronic copy of the proposal (i.e., completion of this document) in Microsoft Word format along with any supplemental documents you wish to include, to the primary contact listed above in Section IV-A. Hard copy proposals are not required.

F. Terms of Proposal Submission

All terms and conditions offered in proposals submitted in response to this RFP must be held open for acceptance for a period of 1 year after submission.

Proposals should be prepared simply and economically, providing a straightforward, concise response to the items within this RFP. **Vendors must use Section V of this RFP as a template for the proposal**.

MSF Eastern Africa will not be liable for any costs or expenses incurred by vendors responding to this RFP or participating in any onsite meetings.

All replies in response to this RFP are the sole property of MSF Eastern Africa. MSF Eastern Africa will not return any proposals; they will be either kept on file or destroyed. Applicants are encouraged to exclude from their response any information that is proprietary to the bidding firm, used without express permission of the owner, or otherwise subject to third party rights.

MSF Eastern Africa reserves the right, in the exercise of its sole discretion, to: (a) reject any or all proposals, in whole or in part, with or without any specific cause, at any time; (b) accept a proposal without further discussion or negotiation; (c) waive any defect or irregularity in a proposal and to accept that proposal when it is otherwise in the interests of MSF Eastern Africa to do so; (d) negotiate directly

with respondents for other terms, prices and conditions deemed proper and reasonable or to protect the interests of MSF Eastern Africa.

All proposals, information, and responses will be incorporated into and made a part of any final agreement between MSF Eastern Africa and the selected vendor. No information should be submitted that cannot be so incorporated into the agreement.

MSF Eastern Africa shall assume no liability for payment of services until the successful applicant is notified and until a contract has been signed by both the vendor and MSF Eastern Africa.

G. Timetable of the Selection Process

Milestone Date*	Project Milestone	Responsible Party
	Proposal distributed to Vendors	MSF Eastern Africa
	Additional Information to Vendors	MSF Eastern Africa
	Submission of Questions	Vendor
	Questions answered for all RFP recipients in writing	MSF Eastern Africa
	Notification of Intent to Respond in writing via email	Vendor
	Proposals Due	Vendor
	Virtual Vendor Meetings	Vendor, MSF Eastern Africa
	Final Negotiations & Vendor Selection	Vendor, MSF Eastern Africa
	Contracting Period	Vendor, MSF Eastern Africa
	Onboarding Period including NDAs	Vendor, MSF Eastern Africa

*Please note all dates are subject to change at the discretion of MSF Eastern Africa

V. VENDOR QUESTIONNAIRE

A. Company Information

1. **Legal name of company**

2. **Year established**

3. **Principal owners of the firm and their percentage of ownership**

4. **Annual revenues for last 3 years**

5. **% of Revenue represented by cumulative revenue of largest two clients**

6. **Breakdown of employees**
   Total:
   Management:
   Technical Support:
   Client Service:

7. **Is there any current or pending litigation against your company or its principals?**

8. **Please provide a copy of your last two audited annual financial statements. If not provided, please explain why.**

9. **Please describe the nature and extent of the contractual liability you are prepared to assume for injuries MSF Eastern Africa or its constituents as a result of breach, negligence, or malfeasance by you or any other participating vendors**

10. **Please inform of any conflicts of interest you may have done business with MSF Eastern Africa**

11. **List any nonprofits who have stopped using the services of your company in the past 18 months along with reason**

12. **Please provide 3 references for organizations that are using the services being proposed for MSF Eastern Africa. These references will be checked only in the event that your company is chosen as a finalist. MSF Eastern Africa reserves the right to contact organizations not included on this list.**

Client Name	Contact Person / Title	Email	Phone Number	Length of time as client

B. Service

13. **What is your related experience in your category? Identify previous experience with others of where you performed similar work.**

14. **Provide sample deliverables and executive summary of proposal, containing synopsis of your approach.**

15. **Propose project plan, including detailed phases, and timing.**

16. **How would MSF Eastern Africa fit into your client portfolio relative to the size and scope of our program? Would your firm be able to service MSF Eastern Africa within the available bandwidth?**

17. **Please describe your firm's organizational structure, account management and their unique qualifications. Specifically:**
    a. Who would be our point(s) of contact? Describe the team, their roles, experience and qualifications. What is the structure for managing accounts?

18. **What is your client onboarding process?**

19. **Please provide detailed information on your strategies and ability to service/support the following items:**
    a. Network equipment from the vendors we have listed in this RFP
    b. Our network setup and configuration
    c. Power inverter system
    d. Servers & virtualization, AD setup, etc.
    e. Microsoft Azure integration with on premise resources

C. Pricing

20. **Please provide your proposed pricing/payment structure along with any assumptions made by your organization in deriving the cost estimates**

21. **What is your firm's incentive to make this potential business relationship successful?**

Pricing Information Contact

Name:	
Title:	
Phone:	
Email:	

22. Please describe the types of ADDITIONAL services you provide that MSF Eastern Africa may wish to take advantage of and indicate fees for each add-on service.

D. Corporate Social Responsibility

23. Does your company have a policy or commitment to green initiatives or environmental responsibilities (i.e., reducing your carbon footprint)?

24. Does your company have any written policy or procedures involving any DEI (Diversity, Equity & Inclusion) initiatives in the hiring and staff retainment process? If so, please describe.