REQUIREMENT SPECIFICATION

TITLE : REQUEST FOR PROPOSAL FOR THE PROVISION OF SUPPLY, DELIVERY AND COMMISSIONING OF SD-WAN, LAN AND WAN TECH REFRESH

1. Introduction

1.1 The National Kidney Foundation ("**NKF**") wishes to appoint service provider (the "**Contractor**") for the provision of supply, delivery and commissioning of SD-WAN, LAN and WAN Tech Refresh.

2. Scope of Service

2.1 There are 2 different scopes of services in this Request for Proposal (RFP):

- Scope of Service for SD-WAN
- Scope of Service for LAN/WIFI Tech Refresh

2.2 The Contractor can quote for one or more of the service(s) stated in the Price Schedule Part A and B. NKF reserves the right to award each part to separate vendors at its sole discretion

2.3 The Contractor shall perform the Services according to the requirements specified in Part A and B, as according to their submission of bid(s) in the Price Schedule.

2.4 The Contractor must have sufficient service liability coverage of at least $1 million. Service liability coverage can include but is not limited to, public liability insurance, workman compensation, etc.

2.5 Sufficiency is determined by NKF. NKF's decision is final.

3. Term of Contract

3.1 The Terms and Conditions as set out in the Conditions of Contract shall form part of the binding contract between the successful Vendor and NKF. The Vendor shall perform the Services according to the requirements specified in Annexes A to F.

3.2 The successful Vendor may be required to enter into further documentation with NKF and shall do so, if ever required by NKF.

3.3 NKF is not obliged to accept and reserves the right to reject the lowest or any quotation, or part or all of any quotation or assign any reason for rejecting any quotation. NKF reserves the right in the exercise of its absolute discretion to accept any part or all of any quotation.

3.4 NKF has the option to terminate in accordance to the Conditions of Contract by giving a written notice of termination to the Contractor at any time prior to the end of the current term.

Company's Stamp & Signature:

3.5 Unless otherwise stipulated by the NKF, all purchases for the Services made during the extended period of this Contract shall be subjected to the terms and conditions hereof (as may be amended, varied, supplemented and/or replaced from time to time), and the Services purchased during such extended period shall be deemed to be Services as defined in this Contract.

4. Compulsory Vendor's Briefing

4.1 Vendors are required to attend a compulsory briefing (either personally or through a company's representative) which will be conducted as follows:

Date: 22 April 2024, Monday
Time: 9.30 am
Venue: NKF Centre, 81 Kim Keat Road, Singapore 328836

4.2 To participate in the briefing session, vendors have to email to raymond.thong@nkfs.org with details on the company's name, attendee's name and email address by 18 April 2024, Thursday before 2.00pm. The meeting details would be emailed to Vendors who had expressed their interest to attend.

5. Submission of RFP Bids

5.1 The quotation submitted by the Contractor shall be as in **Price Schedule**. Each Contractor shall provide the price quote for:

- Price Schedule of Service for SD-WAN (Part A)
- Price Schedule of Service for LAN/WIFI Tech Refresh (Part B)

5.2 The Contractor is required to provide the following information and/or documents to NKF:

5.2.1 Letter of Accreditation from MOH (in accordance to year 2017 standards for MT service or emergency ambulance service)
5.2.2 Relevant Service Liability Insurance(s)
5.2.3 Accredited Certificates
5.2.4 Latest annual report or published accounts;
5.2.5 Original copy of the information on the latest business profile by the Accounting and Corporate Regulatory Authority (ACRA). The date of the business profile should be no more than ninety (90) days from the date of submission;
5.2.6 Track record
5.2.7 Name and contact details of at least three (3) reference customers (Reference check may be conducted on the references provided by the Contractor)
5.2.8 Testimonials from clients
5.2.9 Any other documents relevant to the tender of service

Company's Stamp & Signature:

Annex A

REQUIREMENT SPECIFICATIONS

NKF will be calling an RFP for the Design, Planning, Supply, Delivery, Installation, Configuration, Testing, Migration, Commissioning and Maintenance of a Network Technology Refresh and Software-defined Wide Area Network (SD-WAN) for NKF HQ, IRC and FORTY-FIVE (45) Dialysis Centres across THIRTY-SIX (36) months. The ITQ covers the following areas:

- SD-WAN for NKF HQ, IRC and Disaster Recovery
- SD-WAN for 45 Dialysis Centres/Remote Sites
- 48 port POE switch for HQ, IRC and 45 Dialysis Centres
- 48 port non-POE switch for HQ, IRC and 45 Dialysis Centres
- Access Points for HQ, IRC and 45 Dialysis Centres
- Network Access Control
- Management and Monitoring for Wired, Wireless and SD-WAN
- Professional Services
- Internet Circuits

There will be 2 parts to the Requirement Specifications. Part A is for the SD-WAN, Switches, Access Points, Network Access Control and Professional Services. Part B is for the Internet Circuits.

Vendors can bid for <u>one of the parts or both</u>, but there will be a need to fill Annex E, F and G for each part.

NKF reserves the right to award each part to separate vendors at its sole discretion.

<u>Part A</u>

1. Project General Requirements

The following General Requirements are mandatory. The vendor's submission shall include each requirement stated below in the context of the proposed solution:

1.1. The proposed solution shall provide back-to-back vendor support with OEM vendor.

1.2. The proposed solution shall have separate network architecture based on a multi-tenant network design with zero trust security integration to visualize or monitor as a holistic solution with feature of risk compliance.

1.3. The proposed solution shall be validated and supported by the OEM vendor.

1.4. The proposed solution shall be compatible (for example, Wired and Wireless compatible with Network Access Control, etc.)

1.5. The proposed solution shall be based on current industry and OEM vendor best practices.

1.6. The proposed solution shall be managed by one single Cloud-based Central Management System and supports the latest telemetry-based method to facilitate quick identification of root causes and potential problems of the Wired and Wireless networks.

Company's Stamp & Signature:

1.7. The proposed solution shall be able to provide a quality evaluation system to evaluate the entire network's health and create rankings in seven dimensions: access success rate, coverage, the time required for access, roaming fulfilment rate, capacity, throughput fulfilment rate, and device uptime, and lists deteriorated metrics that affect the rankings.

1.8. The awarded vendor needs to work with the appointed ISP vendor and ensure failover redundancy configuration.

1.9. All proposed equipment shall have a Manufacturer Authorization Letter (MAL) or equivalent documentation from the OEM vendor. NKF reserves the right to reject the equipment or components if the document is not duly furnished.

1.10. The vendor shall cover the design, planning, site survey, mounting, installation, configuration, labelling and testing of all equipment.

1.11. The proposed solution shall support the ability to isolate and troubleshoot network degradation problems by enabling a network administrator to discover an IP flow path, dynamically enable monitoring capabilities on the nodes along the path and collect information on a hop-by-hop basis.

1.12. The vendor is solely responsible to deliver a fully functional solution meeting the specifications described herein. After the award of the contract, the awarded vendor is responsible for any necessary item not brought to the attention of NKF before the award to complete the project by the specifications & design objectives.

1.13. The vendor shall include project management service, or professional service, or the service to design, plan, supply, deliver, install, configure, test, migrate, commission, and maintain the proposed solution.

1.14. All Professional Services for HQ and IRC/DR are to be quoted for weekends after office hours, and remote sites on weekdays after office hours.

1.15. The vendor shall provide all necessary and associated software components (such as Operating Systems, Software Drivers, Firmware, Licenses), accessories (such as Power Cords, Patch Cords), resources (such as manpower to deliver, transport, relocate, mount, dismount, install, patch and label equipment and cables), insurance, custom clearance, and services (including any co-ordination and interfacing works with any third-party contractors) requirement to commission the proposed solution. Such costs shall be deemed to have been included in the base offer.

1.16. The vendor shall provide Maintenance Services over a period of THIRTY-SIX (36) months 24 hours/7days/4hours response for the proposed solution listed in Part A from System Commission date with NKF, with pricing option to extend for an additional TWENTY-FOUR (24) months subject to mutual agreement by both NKF and vendor.

1.17. The vendor shall possess experience and a proven track record in implementing and managing at least five (5) network infrastructure similar type of project with a minimum $1M contract value per contract in the past 5 years in Singapore from 2019 to 2023.

Company's Stamp & Signature:

1.18. The vendor shall provide customer references for past projects. Information is to be listed in Annex I.

1.19. The vendor must be an accredited and certified Partner of the OEM vendor.

1.20. The proposed solutions shall be scalable, resilient and can cater for future expansion.

1.21. The proposed solutions shall have built-in security features such that it can restrict access for different groups of users from various sections of the network.

1.22. The Vendor shall note that all equipment, works and services whether specifically stated in this Specifications, but are necessary for the efficient, stable, and complete satisfactory operation of the setup, shall be included and accounted for in the ITQ submission.

1.23. The Vendor shall be responsible for the provision of temporary storage for the hardware and equipment. The Vendor shall also be responsible for the security of the hardware and equipment prior to the handover to and acceptance by NKF.

1.24. For temporary storage of equipment in NKF premises prior to commissioning, the Vendor is to note that NKF shall not be held responsible for any damaged or missing equipment.

1.25. The Vendor must also ensure no damages to NKF property is incurred in the process of installation. The Vendor shall be held liable for reinstatement of the damaged property.

1.26. At all times, the Vendor shall ensure cleanliness of work area and remove all unwanted components or boxes immediately.

1.27. The Vendor shall plan for all other items, necessary for the execution of the work.

1.28. Maintenance Support Services and Preventive Maintenance for the setup will commence after System Commissioning.

1.29. The Vendor shall list the scope and quote for any Managed Services they wish to provide.

1.30. The Vendor shall quote training courses for THREE (3) users for the products proposed.

1.31. Deployment and features are expected to be standards based. Proprietary products or protocols is not preferred and only considered by NKF should it be the only means to fulfil the requirements.

1.32. The vendor shall provide a price book cost for additional equipment for future expansion in the next THIRTY-SIX (36) plus TWENTY-FOUR (24) months upon contract award.

Estimated quantity of equipment are 30 units of SD-WAN appliances, 15 units of POE switches, 45 units of non-POE switches and 165 units of wireless access points for remote sites. This quantity of devices shall be in addition to the quantity listed in the

Company's Stamp & Signature:

individual specifications listed below and equipment should come with THIRTY-SIX (36) months of Maintenance Services from commission date. NKF will provide 2 months' advance notice to the vendor for the type and quantity of equipment required.

1.33. Tenderer shall complete the Tech Refresh within **10 months** upon award.

2. SD-WAN for NKF HQ, Integrated Renal Centre/Disaster Recovery and 45 Dialysis Centers

2.1. The vendor shall propose a solution to integrate SD-WAN solution based on NKF's current setup with minimal changes to the existing infrastructure. Refer to Annex B for the current Network Diagram.

2.2. The proposed solution shall indicate how Disaster Recovery will work and what is required to implement that.

2.3. The vendor shall include professional services, or the services to design, plan, supply, deliver, install, configure, test, migrate, commission, and maintain the proposed solution, including any changes required to be made on the current infrastructure to fit the proposed solution,

2.4. The proposed SD-WAN appliance shall be able to support 2x1000mbps throughput for HQ and IRC/ Disaster Recovery or 2x500mbps throughput for Dialysis Centers.

2.5. The proposed SD-WAN shall include High Availability for HQ and standalone for all other locations.

2.6. The vendor shall quote the quantity of SD-WAN appliances based on their proposed solution.

2.7. The proposed solution shall support Zero Touch Provisioning for ease of installation, ability to deploy across NKF dialysis centers with minimal to no configuration changes. Devices should automatically show up in Cloud-based Central Management System.

2.8. The proposed solution shall have effective configuration management using a hierarchical configuration model. Allow group configurations to be applied to all devices but at the same time the platform should allow overriding of any configuration items.

2.9. The proposed solution shall support auto-recovery from error configuration push, gateway device should automatically rollback to its previous configuration if an erroneous configuration is pushed making it lose connectivity with the Cloud-based Central Management System.

2.10. The proposed solution shall support management redundancy across any WAN interface.

2.11. The proposed solution shall support site-based topology view to automatically discover other network devices in the same site and discover topology via LLDP.

2.12. The proposed solution shall support site-based monitoring, alerting, and reporting to map all devices to their location and perform monitoring, alerting and reporting on a

Company's Stamp & Signature:

per-site basis.

2.13. The proposed solution shall support application visibility natively display application usage as well as client session information.

2.14. The proposed solution shall support integration with third party tools with inbound and outbound APIs for monitoring, alerting and report generation.

2.15. The proposed solution shall support automated tunnel orchestration, establish secure overlay across any WAN interface.

2.16. The proposed solution shall support automated route orchestration, ability to selectively redistribute routes.

2.17. The proposed solution shall provide full monitoring on orchestrated tunnels and routes through the Cloud-based Central Management System on a Global or Device level.

2.18. The proposed solution shall be designed to scale and capable of handling up to 10,000 SD-WAN devices.

2.19. The proposed solution shall be capable of routing traffic based on L3 to 7 applications, FQDN, source VLAN or even source user-role. For example, guest may not need to access any service behind the corporate tunnel.

2.20. The proposed solution shall support active-active redundancy, SD-WAN gateways shall be able to use each other's WAN circuits connected to their peers.

2.21. The proposed solution shall support WAN payload compression to minimize bandwidth consumption between the Dialysis Centre and HQ.

2.22. The proposed solution shall support Application-based QoS based on role, protocol, port, application.

2.23. The proposed solution shall support monitoring of WAN status, Tunnel status and Path Monitoring status. Providing alerts on the key monitored elements such as Tunnel status, WAN health check and policy compliance.

2.24. The proposed solution shall support stateful firewall for stateful inspection of packets, providing an additional layer of security by tracking the state of network connections. Identifying and controlling traffic based on IP or ports as well as 3100 different applications.

2.25. The proposed solution shall offer the option to deny inbound or outbound connections from malicious IP addresses and allow communication with whitelisted IP addresses.

2.26. The proposed solution shall enhance branch security by providing real-time web content and reputation filtering. Filters can be applied in a per-role basis.

2.27. The proposed solution shall be able to apply consistent security policies to all connected devices without having to break the traffic into different VLANs for each type of device.

Company's Stamp & Signature:

2.28. The proposed solution shall include intrusion detection and prevention systems.

2.29. The proposed solution shall integrate with Zscaler, which is NKF's current Cloud Security Provider for faster delivery and efficient use of bandwidth.

3. Wired Access Switches

3.1. The vendor shall provide SIXTY (60) POE switches and EIGHTY-FIVE (85) non-POE switches.

3.2. The proposed devices shall be FORTY-EIGHT (48) port switches.

3.3. The vendor shall provide THIRTY-SIX (36) months of maintenance for all server farm and core switches listed in Annex D.

3.4. The proposed devices shall support high performance 176 Gbps system switching capacity, 95.2 MPPS of system throughput and up to 40 Gbps stacking bandwidth.

3.5. The proposed devices shall support 802.3af or 802.3at POE Standards and able to detect and power up pre-standard POE device. Support for IEEE 802.3at Power over Ethernet (PoE+) provide up to 30W per port.

3.6. The proposed devices shall support Always on POE, which allows supply of power to POE devices even during reboot and firmware upgrade.

3.7. The proposed devices shall support 8-member stacking and maximum stacking distance of 10KM.

3.8. The proposed devices shall support all the below IEEE standards: IEEE802.1p, IEEE802.1Q, RFC1519 CIDR, RFC1593 OSPFv2, RFC5340 OSPFv3, RFC4252 SSHv6 Authentication, RFC4253 SSHv6 Transport Layer.

3.9. The proposed devices shall support 4094 VLAN IDs.

3.10. The proposed devices shall support Generic Routing Encapsulation (GRE) to enable tunneling traffic over a Layer 3 path.

3.11. The proposed devices shall support switch VXLAN encapsulation (tunneling) protocol for overlay network that enables a more scalable virtual network deployment.

3.12. The proposed devices shall support Uni-directional Link Detection (UDLD) to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected to prevent looping.

3.13. The proposed devices shall support Rapid Per-VLAN Spanning Tree (RPVST+) allows each VLAN to build a separate spanning tree to improve link bandwidth usage; is compatible with PVST+.

3.14. The proposed devices shall support IEEE 802.3ad LACP supports up to 32 LAGs with up to 8-links per LAG; and provides support for static or dynamic groups and a user-selectable hashing algorithm.

Company's Stamp & Signature:

3.15. The proposed devices shall support traffic prioritization (802.1p), strict priority (SP) and deficit weighted round robin (DWRR).

3.16. The proposed devices shall be able to limit transmission rates of egressing frames on a per-queue basis using Egress Queue Shaping (EQS).

3.17. The proposed devices shall support rate limiting sets per-port ingress enforced maximums and per port, per-queue minimums.

3.18. The proposed devices shall support built-in programmable and easy to use REST API interface.

3.19. The proposed devices shall support configuration rollback, multiple configuration files can be stored to flash image and allow rollback of any configuration without requiring reboot.

3.20. The proposed devices shall support Secure Sockets Layer (SSL) which encrypts traffic, allowing secure access to the browser-based management GUI in the switch.

3.21. The proposed devices shall support cloud-based management for unified network operations.

3.22. The proposed devices shall be capable to receive the security setting such as user-role, access control list from Network Access Control, this allows the administrator to create the policy only once and deploy the same policy across the entire network.

3.23. The proposed devices shall provide direct access to the OEM vendor support website to download all future software or operating system releases (when available) until the end of support of the product.

3.24. The proposed devices shall support Routing In formation Protocol version 2 (RIPv2) and RIPng.

3.25. The proposed devices shall support jumbo frame size of up to 9198 bytes.

3.26. The proposed devices shall support VXLAN encapsulation (tunnelling) protocol for overlay network that enables a more scalable virtual network deployment.

3.27. The proposed devices shall support Internet Group Management Protocol IGMPv1, v2 and v3 to control and manage the flooding of multicast packets in a Layer 2 network.

3.28. The proposed devices shall support IGMP snooping allowing multiple VLANs to receive the same IPv4 multicast traffic, lessening network bandwidth demand by reducing multiple streams to each VLAN.

3.29. The proposed devices shall support any-source multicast, IGMP utilizes Any-Source Multicast (ASM) to manage IPv4 multicast networks.

3.30. The proposed devices shall have integrated trusted platform module (TPM) for platform integrity.

Company's Stamp & Signature:

3.31. The proposed devices shall support Access Control List (ACL) for both IPv4 and IPv6, also provide filtering based on the IP field, source or destination IP address or subnet, and source or destination TCP or UDP port number on a per-VLAN or per-port basis.

3.32. The proposed devices shall support Remote Authentication Dial-In User Service (RADIUS) and ensure critical devices are still allowed network access during RADIUS server failure.

3.33. The proposed devices shall support Terminal Access Controller Access-Control System (TACACS+).

3.34. The proposed devices shall support Control Plane Policing sets rate limit on control protocols to protect CPU overload from DOS attacks.

3.35. The proposed devices shall support RadSec enables RADIUS authentication and accounting data to be passed safely and reliably across insecure networks.

3.36. The proposed devices shall support ICMP throttling, prevent ICMP denial-of-service attacks by enabling any switch port to automatically throttle ICMP traffic.

3.37. The proposed devices shall support tunneling of traffic from switches to transport user traffic to a Layer 7 firewall to enhance security, visibility, and performance, providing automated device profiling and role-based access control.

3.38. The proposed devices shall support multiple PoE allocation methods (allocation by usage or class with LLDP and LLDP-MED) to allocate PoE power for more efficient power management and energy savings.

3.39. The proposed devices shall have an analytic engine to monitor and analyze events that can impact network health:

1	Easy access to all network state information allows visibility and analytics
2	Rest APIs and Python scripting for fine-grained programmability of network tasks.

3.40. The proposed devices shall support continuous telemetry data with WebSocket subscriptions for event driven automation.

3.41. The proposed devices shall support downloading of Analytic Agent from the OEM vendor to extend the function and features of the switches in terms of visibility, analytics, and automation.

4. Wireless Access Points

4.1. NKF requires a total of TWO HUNDRED SEVENTY (270) Wireless Access Points.

4.2. ** For Vendors that will proposing HPE Aruba Wireless Access Points only:

4.2.1. Vendors have the option to only replace the existing ONE HUNDRED TEN (110) Aruba 305 Access Points.

Company's Stamp & Signature:

4.2.2. In-lieu of replacing the existing fleet of HPE Aruba 505 and HPE Aruba 615 Wireless Access Points listed in Annex D, vendors must provide THIRTY-SIX (36) months of maintenance services.

4.3. The proposed devices shall have comprehensive dual radio or tri-band coverage across 2.4 GHz, 5GHz, and 6GHz (dual concurrent) to deliver up to 3.6 Gbps combined peak data.

4.4. The proposed devices shall have 802.11ax 2x2 MIMO radios deliver a combined peak data rate of up to 3.6 Gbps when configured for concurrent 5 GHz and 6 GHz operation.

4.5. The proposed devices 5 GHz radio shall support two spatial stream Single User (SU) MIMO for up to 1.2 Gbps wireless data rate with 2SS HE80 802.11ax client devices.

4.6. The proposed devices 2 GHz radio shall support two spatial stream Single User (SU) MIMO for up to 574 Mbps wireless data rate with 2SS HE40 802.11ax client devices (287Mbps for HE20).

4.7. The proposed devices 6 GHz radio shall support two spatial stream Single User (SU) MIMO for up to 2.4 Gbps wireless data rate with 2SS HE160 802.11ax client devices.

4.8. The proposed devices shall support both downlink and uplink MU-MIMO in 6 GHz and 5 GHz, downlink only in 2.4 GHz.

4.9. The proposed devices shall support up to seven 160 MHz channels in 6 GHz support low-latency, bandwidth-hungry applications like high-definition video.

4.10. The proposed devices shall support for up to 512 associated client devices per radio and up to 16 BSSIDs per radio (limited to 4 for the 6 GHz radio).

4.11. The proposed devices shall support the below frequency bands (country-specific restrictions apply):

1	2.400 to 2.4835GHz ISM
2	5.150 to 5.250GHz U-NII-1
3	5.250 to 5.350GHz U-NII-2A
4	5.470 to 5.725GHz U-NII-2C
5	5.725 to 5.850GHz U-NII-3/ISM
6	5.850 to 5.895GHz U-NII-4
7	5.925 to 6.425GHz U-NII-5
8	6.425 to 6.525GHz U-NII-6
9	6.525 to 6.875GHz U-NII-7
10	6.875 to 7.125GHz U-NII-8

4.12. The proposed devices shall support Dynamic Frequency Selection (DFS) optimizes the use of available RF spectrum in the 5 GHz band.

4.13. The proposed devices shall support the below radio technologies:

1	802.11b: Direct-sequence spread-spectrum (DSSS)
2	802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM)

Company's Stamp & Signature:

3	802.11ax: Orthogonal frequency-division multiple access (OFDMA) with up to 8 resource units

4.14. The proposed devices shall support the below modulation types:

1	802.11b: BPSK, QPSK, CCK
2	802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM and 256- QAM
3	802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM and 1024-QAM
4	802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM and 1024-QAM

4.15. The proposed devices shall support the below data rates (Mbps):

1	802.11b: 1, 2, 5.5, 11
2	802.11a/g: 6, 9, 12, 18, 24, 36, 48, 54
3	802.11n: 6.5 to 600 (MCS0 to MCS31, HT20 to HT40), 800 with 256-QAM
4	802.11ac: 6.5 to 1,733 (MCS0 to MCS9, NSS = 1 to 4, VHT20 to VHT160(80+80)); VHT80); 2,167 with 1024-QAM
5	802.11ax (2.4GHz): 3.6 to 1,147 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE40)
6	802.11ax (5GHz): 3.6 to 2,402 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE160(80+80)) HE80)
7	802.11ax (6GHz): 3.6 to 4,804 (MCS0 to MCS11, NSS = 1 to 4, HE20 to HE160)

4.16. The proposed devices shall be able to configure Transmit Power in increments of 0.5dBm.

4.17. The proposed devices shall support Maximum (aggregate, conducted total) transmit power) limited by local regulatory requirements) per radio or band (2.4 GHz / 5 GHz / 6 GHz): +24 dBm (18 dBm per chain).

4.18. The proposed devices shall support built in GPS receivers and intelligent software enable APs to self-locate and act as reference points for accurate indoor location measurement.

4.19. The proposed devices shall support 2.5 Gbps Smart Rate Ethernet port to minimize wired bottlenecks.

4.20. The proposed devices shall support unified AP with flexibility to be deployed in either controller based or controller-less networks.

4.21. The proposed devices shall have uplink Ethernet port with:

1	Auto-sensing link speed (100/1000/2500 BASE-T) and MDI/MDIX.
2	2.5Gbps speeds comply with NBase-T and 802.3bz specifications.
3	Backwards compatible with 100/1000 Base-T.

4.22. The proposed devices shall support direct DC power and Power over Ethernet (POE).

Company's Stamp & Signature:

4.23. The proposed devices shall be able to actively measure the power utilization of an AP and dynamically apply restrictions depending on the available power budget and actual consumption.

4.24. The proposed devices shall support priority handling and policy enforcement for unified communication applications, including Microsoft Teams with encrypted videoconferencing, voice, chat, and desktop sharing.

4.25. The proposed devices shall support deep packet inspection to classify and block, prioritize, or limit bandwidth for thousands of applications in a range of categories.

4.26. The proposed devices shall have built-in Trusted Platform Module (TPM) for enhanced security and anti-counterfeiting.

4.27. The proposed devices shall have integrated wireless intrusion protection offering threat protection and mitigation and eliminates the need for separate RF sensors and security appliances.

4.28. The proposed devices shall have IP reputation and security services to identify, classify, and block malicious files, URLs and IPs providing comprehensive protection against advanced online threats.

4.29. The proposed devices shall have automatic thermal shutdown and recovery function.

4.30. The proposed devices shall support low-density parity check (LDPC) for high-efficiency error correction and increased throughput.

4.31. The proposed devices shall support Transmit beamforming (TxBF) for increased signal reliability and range.

4.32. The proposed devices shall support 802.11ax Target Wait Time (TWT) to support low-power client devices and 802.11mc Fine Timing Measurement (FTM) for precision distance ranging.

4.33. The proposed devices shall have an integrated omnidirectional antenna with roughly 30 to 40 degrees down-tilt and peak gain of 2.6 dBi.

4.34. The proposed devices shall have visual indicators (four multi-color LEDs): System (1x) and Radio (3x) status.

4.35. The proposed devices shall have a reset button for factory rest, LED mode control (normal or off), serial console interface (proprietary, micro-B USB physical jack) and Kensington security slot.

4.36. The proposed devices shall have Mean Time Between Failure (MBTF) – 540,000 hours (62 years) at +25 C operating temperature.

4.37. The proposed devices shall support the below regulatory compliance:

Company's Stamp & Signature:

1	FCC/ISED
2	CE Marked
3	RED Directive 2014/53/EU
4	EMC Directive 2014/30/EU
5	Low Voltage Directive 2014/35/EU
6	UL/IEC/EN 60950
7	IEC/EN 62368-1
8	EN 60601-1-1, EN60601-1-2

5. Network Access Control

The vendor is to propose a Network Access Control solution to replace the existing Aruba Clearpass C2000. The current solution is a total of THREE (3) appliances; TWO (2) in HQ and ONE (1) in IRC as a single cluster.

5.1. The proposed solution shall be a single platform approach that combines AAA, NAC, BYOD and Guest Access by incorporating identify, health, physical or device information, and conditional elements into one set of policies.

5.2. The proposed solution shall have the ability to scale up to 25,000 devices per appliance or virtual appliance and 1 million unique endpoint authentications.

5.3. The proposed solution shall be agnostic to current wired, wireless and VPN network in NKF today.

5.4. The proposed solution shall have shell protected by CLI providing configuration for base application settings.

5.5. The proposed solution shall provide disk or file encryption.

5.6. The proposed solution shall have the ability to mix and match virtual and hardware appliances in one deployment.

5.7. The proposed solution shall be deployable in an out-of-band model and support for clustering with N+1 redundancy model.

5.8. The proposed solution shall be available as a hardened appliance or VM machine.

5.9. The proposed solution shall have a web-based, interface that includes several productivity tools such as a configuration wizard and pre-configured policy templates.

5.10. The proposed solution shall support any type of networking equipment (wired, wireless, VPN) and a variety of authentication methods (802.1x, MAC auth, Web auth).

5.11. The proposed solution shall be able to take advantage of a phased implementation approach by starting with one element of access management (role-based) and later incorporating added security measures (endpoint health, wired port security)

Company's Stamp & Signature:

5.12. The proposed solution must incorporate a complete set of tools for reporting, analysis, and troubleshooting. Data from access transaction can be organized by customizable data elements and used to generate graphs, tables, and reports. Must correlate and organize user, authentication, and device information together for ease of troubleshooting, tracking, etc.

5.13. The proposed solution must have fully integrated support for Microsoft NAP allowing health and posture checks on Windows endpoint without the need to install an agent.

5.14. The proposed solution shall have APIs that are available to extend the system to support different authentication protocols, identity stores, health evaluation engines and port and vulnerability scanning engines.

5.15. The proposed solution shall have Restful APIs to interact with leading MDM or EMM vendors within the base license.

5.16. The proposed solution shall support agent and agentless health checking methods and be available as a permanent or dissolvable health agent for Windows, Linux, and Macintosh endpoint platforms. In additional to authenticating the user, the solution must gather granular information about the endpoint devices, perform advanced health checks on Windows platform (services, processes, peer to peer apps, registry keys, USB device usage, Windows Hot Fixes, patch management agents), and perform standard health checks on Linus and Mac platforms (Anti-virus, Anti-spyware, Firewall).

5.17. The proposed solution must be an easy-to-deploy hardware or virtual appliance platform that utilizes identity-based policies to secure network access and includes an integrated set of capabilities bundled under one policy platform:

1	Full AAA server – RADIUS and TACACS+
2	Device Profiling
3	Built-in Guest Management and Device or User On-boarding
4	Web-based Management interface with Dashboard
5	Reporting and Analysis with custom Data Filters
6	Data Repository for User, Device, Transaction information
7	Rich policies using identity, device, health, or conditional elements.
8	Deployment and implementation tools.

5.18. The proposed solution must support flexible licensing model based on required functionality (i.e. Access, Posture, Guest Access)

5.19. The proposed solution AAA framework must allow for the complete separation of Authentication and Authorization sources. For example, authentication against Active Directory but authorization against an external SQL database.

5.20. The proposed solution authentication or authorization shall support LDAP, AD, Kerberos, Token Server, SQL compliant database.

Company's Stamp & Signature:

5.21. The proposed solution shall support multiple methods for device identification and profiling such as:

1	Integrated, network based, device profiler utilizing collection via SNMP, DHCP, HTTP, AD, ActiveSync
2	Endpoint audit via NESSUS or NMAP scanning.

5.22. The proposed solution shall support the below policy creation tools and policy model shall support incorporation of several contextual elements including identity, endpoint health, device, authentication methods and types, and conditions such as location, time, day, etc.:

1	Pre-configured templates
2	Wizard based interface
3	LDAP browser for quick look-up of AD attributes
4	Policy simulation engine for testing policy integrity

5.23. The proposed solution shall support the following enforcement methods:

1	VLAN steering via RADIUS IETF attributes and VSAs
2	VLAN steering and port bouncing via SNMP.
3	Access Control Lists – both statically defined filter-ID based enforcement, as well as dynamically downloaded ACLs
4	Roles or any other vendor-specific RADIUS attribute supported by the network device.
5	Agent-based enforcement – bouncing a managed interface and sending custom messages. Also, control access to different networks via whitelist and blacklist.

5.24. The proposed solution shall be able to join multiple Active Directory domains and forest to facilitate 802.1x PEAP authentication and query seamlessly.

5.25. The proposed solution shall be able to support complex PKI deployment where TLS authentication requires validating client certificate from multiple CA trust chain. Must also support AAA server certificate being signed by external CA whilst validating internal PKI signed client certificates.

5.26. The proposed solution shall support Automatic Sign On (ASO) which captures the user's initial 802.1x credentials and uses these to automatically sign the user into their SAML supported applications.

5.27. The proposed solution shall support SAML capabilities to act as an identity provider (IDP) for the principal user.

5.28. The proposed solution shall support profiling capabilities to offer full visibility of the devices present on the network.

Company's Stamp & Signature:

5.29. The proposed solution shall have the ability to be clustered in any combination via local and remote network connections providing unlimited scale, redundancy, and access load balancing.

5.30. The proposed solution shall support several deployment modes including centralized, distributed, or mixed.

6. Cloud-based Central Management System

6.1. The proposed solution shall provide cloud-based management and control of wireless, wired, and SD-WAN for simplified operations.

6.2. The proposed solution shall have a network fabric orchestration, intent-based policy engine and access controls for unified policy management, automated network provisioning and zero-trust security at scale.

6.3. The proposed solution shall have Machine Learning AI-powered features for faster troubleshooting and continuous network optimization.

6.4. The proposed solution shall have the ability to integrate with user simulation sensors to proactively monitor and improve the end-user experience.

6.5. The proposed solution shall come with advanced IPS/IDS threat defense management feature.

6.6. The proposed solution shall come with Machine-learning AI that automates common troubleshooting activities, reducing IT support tickets and associated costs. Solution shall be based on machine learning models that are consistently trained with network performance data collected across every vertical, market segment and network type.

6.7. The proposed solution shall have core AI components that include:

1	Automatically surface and diagnose an array of common network-impacting issues by using dynamic, per-site baselines that are continuously tuned as conditions change.
2	Uses event-driven automation to collect diagnostics, post them to a shared location, generate a ticket in tools such as Ticketing Helpdesk System, and even notify TAC for proactive customer support.
3	Recommendation to troubleshoot issues.

6.8. The proposed solution shall have monitoring capabilities not limited to:

1	Network Health – Gain broad visibility into network-wide performance, and drill into specific sites with summaries of device utilization, configuration compliance, and other statistics.
2	Application Visibility – Monitor application health across the network, helping to ensure that critical services receive priority traffic while tracking and enforcing acceptable usage by site, device, or location.

Company's Stamp & Signature:

3	Analytics – A consolidated view of how VoIP applications are performing with mean opinion scores (MOS) and insights into potential RF performance and capacity issues.
4	Client Health – Delivers a multitude of details on devices connected to the network, including insights into client performance, connectivity status, physical location, and the data path.
5	AI-based Connectivity Insights – Automatically identify potential Wi-Fi connectivity issues tied to DHCP, DNS, authentication failures, and more.
6	For Wired Networks, IT operations gain visibility into the health and utilization of both individual and stacked switches. This includes port status, PoE consumption, VLAN assignments, device and neighbor connections, power status, and more-with built-in alerts and events that accelerate wired network troubleshooting.

6.9. The proposed solution shall provide an integrated topology view for graphical representation of gateways and details per site.

6.10. The proposed solution shall provide monitoring of WAN circuit health, bandwidth availability, and tunnel status for each site.

6.11. The proposed solution shall provide quality of experience (QoE) scores for SaaS applications with drilldowns for root cause analysis.

6.12. The proposed solution shall provide WAN orchestration for managing routing preferences across branches and data centres.

7. Security & Architectural Requirements

7.1. Security patches should be validated by the Product Vendor before installation.

7.2. Security patches should be scanned for malware before installation.

7.3. The Vendor shall ensure up-to-date security patches are installed prior to commissioning.

7.4. Network redundancy should be designed to avoid single point of failure.

7.5. Network topology showing the physical and logical assets should be documented.

7.6. Configuration changes should be tested before deployment into production environment.

7.7. Impact assessment of configuration changes should be performed prior to deployment.

7.8. Configuration changes should be validated by the Vendor prior to deployment.

Company's Stamp & Signature:

7.9. Roll-back plan should be established before configuration changes are deployed.

7.10. Configuration changes should be authorised prior to deployment.

7.11. Configuration changes should be performed during scheduled maintenance period.

7.12. Production systems should be monitored after configuration changes to ensure they continue to operate as intended.

7.13. The overall solution should include Disaster Recovery setup and documented steps on tasks required to activate and implement Disaster Recovery.

Company's Stamp & Signature:

Part B

1. Internet Circuits

NKF requires two (2) internet circuits going to different Point of Presence (POP) for each location for redundancy purposes.
Internet Service Providers (ISP) that can provide such internet connectivity are welcome to submit two bids. NKF reserves the right to award the internet circuits to different ISP.

The following requirements is per circuit.

1.1. The ISP is to provide fiber optic internet connectivity.

1.2. The ISP will provide the following:

1	1000mbps internet connectivity with 30 usable public IP for NKF HQ and IRC
2	500mbps internet connectivity with 1 usable public IP for 45 Dialysis Centres

* Refer to Annex C for list of locations

1.3. The circuit should have the following parameters:

1	Symmetric throughput
2	<250ms latency
3	Packet Loss/Drop of <1.0%
4	Mean Time to Restore of 4 hours monthly
5	Real Time, Hourly, Daily, Weekly and Monthly performance report

1.4. The ISP shall indicate the service uptime of the internet circuits proposed.

1.5. The ISP shall state the liability/penalty should the service fail SLA.

1.6. The ISP will indicate if the proposed circuit has active outage monitoring as well as any customer notification and/or active resolution of problem.

1.7. Any new fiber installations required will be done on Sunday.

1.8. The ISP shall provide pricing for the internet circuits with or without managed routers including maintenance services according to the price schedule.

1.9. The ISP shall provide details of POP location for each circuit.

1.10. The ISP shall provide technical support contact details with 24/7 availability and onsite support to resolve any circuit issues.

1.11. The provided circuit shall be scalable to upgrade bandwidth when required by NKF.

1.12. The internet circuits shall be billed monthly or quarterly.

1.13. The ISP shall provide the cost breakdown, including Monthly Recurring Cost (MRC), One-Time Cost (OTC) and hardware costs (if any) in Annex F.

Company's Stamp & Signature:

1.14. The vendor shall provide a price book cost for any additional circuit at 500mbps required for future expansion in the next THIRTY-SIX (36) plus TWENTY-FOUR (24) months upon contract award.

1.15. The vendor shall also provide upgrade options in the price schedule for upgrading from 500mbps to 1000mbps and from 1000mbps to 2000mbps.

1.16. The contract shall be awarded for THIRTY-SIX (36) months with an option to renew for a further TWENTY-FOUR (24) months subject to satisfactory performance of internet services at same terms & conditions of the existing contract.

Accepted By:

Authorized Signature: _____ Date: _____

Signatory Name: _____ Signatory Title: _____

Telephone Number: _____ Contractor's Name: _____

Email Address: _____ Contractor's Stamp: _____

Company's Stamp & Signature:

Annex B

Current Network Diagram

Hardcopy will be provided during mandatory briefing session.

Company's Stamp & Signature:

Annex C

Location of all sites

Location	Address
HQ	81 Kim Keat Road S (328836)
IRC/DR	500 Corporation Road S (649808)
ADT	BLK 761 Woodlands Ave 6. #01-108. S (730761)
ALJ	BLK 102 Aljunied Crescent. #01-265. S (380102)
AM3	BLK 633 Ang Mo Kio Ave 6. #01-5155. S (560633)
AM2	BLK 565 Ang Mo Kio Ave 3. #01-3401. S (560565)
BB2	BLK 113A Bukit Batok West Ave 6. #01-01. S (651113)
BI1 *	BLK 213 Bidadari Park Drive Level 3. S (360213)
BD2	BLK 105 Bedok North Ave 4. #01-2168 , S(460105)
BED	BLK 27 New Upper Changi Rd. #01-694 S (462027)
BM2	BLK 128 Bukit Merah View. #01-22 S (150128)
BP1	BLK 274 Bangkit Rd. #01-54. S (670274)
BP2	BLK 275 Bangkit Rd. #01-96. S(670275)
CLE	BLK 326 Clementi Ave 5. #01-175. S (120326)
GMH	BLK 1 Ghim Moh Road,#01-358. S (270001)
HG1	BLK 114 Hougang Ave 1. #01-1298. S (530114)
HG2	BLK 628, Hougang Ave 8. #01-108. S (530628)
JE1	BLK 240C Jurong East Ave 1. #01-01. S (603240)
JW1	BLK 744 Jurong West St 73. #01-19. S (640744)
JW2	Blk 940 Jurong West Street 91. #01-441. S (640940)
KKT	81 Kim Keat Rd. Level 3. S (328836)
KLA	BLK 43 Bendemeer Rd. #01-1018. S (330043)
MSD	BLK 204 Marsiling Drive. #01-188. S (730204)
MUN	Blk 53 , Kim Keat Rd #05-01 Mun Hean Building
PNG	BLK 681 Punggol Drive. #02-02. S (820681).
PG2 *	1 Punggol Drive #04-08. S (828629)
PR2	BLK 427 Pasir Ris Drive 6. #01-35/43. S (510427)
PSR	BLK 180 Pasir Ris St 11. #01-06. S (510180)
QT1	BLK 55 Strathmore Ave. #01-145. S (140055)
SK1	1 Anchorvale Street #01-36, Sengkang Community Hospital S (544835)
SK2 *	BLK 465 Fernvale Road #01-07. S (790465)
SMI	BLK 101 Simei St 1. #01-892. S (520101)
SRG	BLK 201 Serangoon Central. #01-30. S (550201)
TM1	BLK 935 Tampines St 91. #01-333. S (520935)
TM2	BLK 271 Tampines St 21. #01-99. S (520271)
TP1	BLK 225 Toa Payoh Lorong 8. #01-54. S (310225)
TP2	200 Toa Payoh Lorong 2. #03-01. S (319642)
TWY	BLK 113 Teck Whye Lane. #01-666. S (680113)
UBK	Blk 19 Upper Boon Keng Rd #01-1220. S (380019)
URD	BLK 311 Ubi Ave 1. #01-383 S (400311)
WCR	Blk 701 West Coast Rd #01-323. S (120701)
WD1	BLK 825 Woodlands St 81. #01-30. S (730825)
WD2	BLK 365 Woodlands Ave 5. #01-490. S (730365)
YS1	BLK 203 Yishun St 21. #01-239. S (760203)
YS2	BLK 639, Yishun St 61. #01-168, S (760639)
YS3	BLK 840 Yishun St 81. #01-382, S(760840)
YS4	2 Yishun Central 2. #03-01 Yishun Community Hospital, S(768024)

* Unit number subject to change as it is a new site

Company's Stamp & Signature:

Annex D

Inventory

Inventory will be provided during mandatory briefing session

Company's Stamp & Signature:

Annex E

Customer Reference			
No	**Name**	**Company**	**Email**
1			
2			
3			

Company's Stamp & Signature:

Annex F

PROJECT REQUIREMENT

All requirement mentioned herewith are mandatory

S/N	Requirement	Comply (Yes / No / NA)	Remarks
1	**Specifications** As specified in **Project General Specifications.**		
2	**Specifications** As specified in **SD-WAN for NKF HQ, Integrated Renal Centre/Disaster Recovery and 45 Dialysis Centers**		
3	**Specifications** As specified in **Wired Access Switches**		
4	**Specifications** As specified in **Wireless Access Points**		
5	**Specifications** As specified in **Network Access Control**		
6	**Specifications** As specified in **Cloud-based Central Management System**		
7	**Specifications** As specified in **Security & Architectural Requirements**		
8	**Specifications** As specified in **Internet Circuits**		

Accepted By:

Authorized Signature: _____ Date: _____

Signatory Name: _____ Signatory Title: _____

Telephone Number: _____ Vendor's Name: _____

Email Address: _____ Vendor's Stamp: _____

Company's Stamp & Signature: