

REQUIREMENT SPECIFICATION

TITLE : REQUEST FOR PROPOSAL FOR THE PROVISION OF SERVER INFRASTRUCTURE TECH REFRESH FOR NKF

1. Introduction

- 1.1. The National Kidney Foundation (NKF) Department of Information Technology is requesting proposals for the provisioning of a complete Technology Refresh and Migration for the Information Technology server infrastructure, maintenance, and upkeep at 81 Kim Keat Road and 500 Corporation Road.

2. Scope of Service

- 2.1 We have a main office located at 81 Kim Keat Road housing our HQ server room. The scope of this RFP covers the server and network technology and supporting software at the main office and our disaster recovery site, situated at 500 Corporation Road; migration and upgrading from current hardware and software; as well as the support to NKF IT staff throughout the migration process.
- 2.2 The Contractor shall perform the Services according to the requirements specified in Annex A to F, as according to their submission of bid(s) in the Price Schedule.
- 2.3 Sufficiency is determined by NKF. NKF's decision is final.

3. Term of Contract

- 3.1 The Contractor shall complete the server infrastructure tech refresh within **two (2)** months and providing the Services over a period of **sixty (60)** months, tentatively starting from November 2024.
- 3.2 NKF has the option to terminate in accordance with 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.
- 3.3 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** online briefing session (either personally or through a company's representative) on the date and time specified below:

Date: 9 May 2024, Thursday
Time: 9.30 am
Mode: **Online**, Microsoft Teams

- 4.2 To participate in the online briefing session, Vendors are required to email to raymond.thong@nkfs.org with details on the company's name, attendee's name and email address by **7 May 2024, Tuesday before 12pm**. 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**.
- 5.2 The Contractor is required to provide the following information and/or documents to NKF:
- 5.2.1 Latest annual report or published accounts;
 - 5.2.2 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;
 - 5.2.3 Any other documents relevant to the tender of service

SPECIFICATIONS

1. Project Scope of Work

- 1.1 The Contractor shall propose and quote the following items in accordance to the requirements in this RFP:
- a) Supply, Delivery, Installation, testing, commissioning, and Warranty Support (Including 5 years of license, hardware & software maintenance, and support for all components of the proposed solution) for **servers, storage and network equipment**.
 - i) The proposed quantity of servers in PROD environment should cater for HA with resiliency of 1 server minimally with no impact to production workload.
 - ii) The proposed quantity of servers in DR environment should cater for HA with resiliency of 1 server minimally.
 - iii) The proposed solution should include all licenses required for 5 years.
 - b) Supply, Delivery, Installation, testing, commissioning, and Warranty Support (Including 5 years of license, hardware & software maintenance, and support for all components of the proposed solution) for 4 units of server farm switches. The proposed switches must minimum capable to support 10G interface speed.
 - c) Professional Services:
 - Part A: Replace & Migrate existing production End-Of-Life Cisco N9K to new proposed server farm switches (Production site + DR site)**
 - i) Hardware Staging, mounting, labelling, and device interconnection to network.
 - ii) Firmware upgrade of the switches to latest.
 - iii) Migrate and merge existing network configurations to new devices.
 - iv) Setup and configure 4 x new switches.
 - v) Configure hostname and network VLAN and IP.
 - vi) Setup Routing and switching.
 - vii) Provide and conduct switch hardening.
 - viii) Conduct UAT.
 - Part B: Server and Storage (Production site + DR site)**
 - i) Hardware Staging, mounting, labelling, and device interconnection to network.
 - ii) Firmware upgrade to latest.
 - iii) IP & Hostname Configurations

- iv) Install licenses and update to latest.
- v) Configure email notifications.
- vi) Create 1 VM for test purpose.
- vii) Failover and VM migration Test
- viii) Migrate all 200 VMs from 3 environments (PROD, DR & UAT)
- ix) Setup Micro-segmentation for at least 3 use cases.
- x) Enable and perform data-at-rest encryption (DaRE) at the cluster level using software ONLY.
- xi) Verify and confirm virtual machines resumes normal operations.
- xii) Setup replication for up to 75 VMs from PROD to DR for Disaster Recovery.
- xiii) Configure all network interface, storage, folder mapping for all protected VMs.
- xiv) Configure DR Failover automation runbooks for all protected VMs.
- xv) Perform 1 x DR Test exercise to initiate the failover and recovery (On weekend) – To be done post migration.
- xvi) Configure all fixes/changes required if identified during DR Test exercise.
- xvii) Provide manpower to standby onsite during 1 x actual DR exercise. (On weekend) – To be done post DR Test exercise.

2. Background

2.1 Current Environment

- Current solution has 5 servers running virtualized platform (VMware), a storage system on the main site as well as 2 servers running the same platform at Disaster Recovery site.
- Domain controllers are running Windows Server 2022 Datacenter 64-bit Operating Systems.
- Utilizing storage-based snapshot replication for site-to-site replication via point-to-point dedicated link between main site and DR.
- VMWare and ESXi servers are configured on both sites to provide High Availability within sites and no fail-over between sites.
- Current storage utilization at main site is at approximately 70% of effective usable capacity of 100TB.
- Current environment is split into 3 clusters (Production, Disaster Recovery, UAT).

For the purpose of this proposal, we will relocate UAT cluster to reside on Disaster Recovery hardware.

1. Technical Specifications

1.1 Functional Requirements

- 1.1.1 The participating Suppliers are required to propose the supply, commission, installation, implementation, testing and configuration of server infrastructure solution.
- 1.1.2 The proposed solution shall comprise integrated hyperconverged nodes that deliver virtual compute (CPU and memory) resources in the cluster for PROD and DR environment.
- 1.1.3 The proposed hardware shall come with Five (5) Years warranty support with 24x7x4 coverage.
- 1.1.4 The proposed software shall come with Five (5) Years warranty support with 24x7x4 coverage.
- 1.1.5 The proposed hardware platform must be certified to run the proposed virtualization platform.
- 1.1.6 The proposed hardware must support logging a support call using the same portal as the virtualization platform.
- 1.1.7 The virtualization platform must have the ability to support multi-hypervisors like VMware, KVM based hypervisor(AHV) and Microsoft Hyper-V (without the need of SCVMM).
- 1.1.8 The solution shall have high-availability platform with automatic failover to minimise disruptions and downtime to VMs due to any hardware maintenance, patching or failure. The solution shall ensure there is no single point of failure for the virtualization implementation.
- 1.1.9 The solution shall leverage Flash devices (e.g. Solid-State drives) minimally for caching and tiering content during read/write operations. Persistent data storage may consist of magnetic disks (e.g. NLSAS, SAS, SATA); this is to ensure that superior performance is maintained with a good balance in cost.
- 1.1.10 If the proposed solution consists of magnetic disks, the technology shall also support intelligent Distributed Data Tiering, which will intelligently place data in the optimal storage tier (flash or HDD) to yield the fastest possible performance.
- 1.1.11 The proposed solution shall support both compression and deduplication (both inline and post) to gain more logical storage capacity when needed on selected logical storage containers and not across the entire cluster – this ensures that workloads which do not benefit from data reduction do not go through a data reduction algorithm cycle.

- 1.1.12 The supplier shall ensure that the proposed solution supports the needs of high IOPs and low latency workloads. The supplier must ensure that virtual machines can be pinned to reside on Flash devices only within a Hybrid Flash deployment – the supplier must provide documents as part of the proposal for evaluation which show how this can be achieved in a Hybrid environment.
- 1.1.13 As nodes will be added into the resource farm at different points in time, the supplier needs to ensure that the design supports intermix of different hardware configurations and models within the same cluster. Server models need not be of a similar resource configuration from a storage, memory, and CPU perspective. This should include different CPU generations as well.
- 1.1.14 Locality should also be implemented whereby the system will always attempt to place a workload's data on the same node where the workload is executed upon, thus reducing network traffic, and making best use of investments in the network fabric.
- 1.1.15 The proposed solution must ensure continuous security compliance. It should be able to provide full details of the security baseline to address various vulnerability assessments and lock downs done on the components within the technology.
- 1.1.16 The proposed solution must provide a machine-readable Secure Technical Implementation Guide (STIG) that supports the SCAP standard and allows automated compliance checking, supporting the DIACAP process, installed by default. It should support self-healing of security hardened settings within the STIG, reverting any changed settings to the as-desired baseline.
- 1.1.17 The proposed solution shall be able to support software-based encryption if necessary.
- 1.1.18 The software-based encryption must not affect storage efficiency features such as compression, deduplication, snapshot, and cloning.
- 1.1.19 The software-based encryption must be able to support disk level encryption.
- 1.1.20 The proposed solution shall be able to work with external key managers if needed.
- 1.1.21 The proposed solution shall leverage a complete software-based solution so that all intelligence of managing the hardware is based on a software defined storage approach.
- 1.1.22 To support the need of site resiliency protection mechanism, the proposed technology should support storage replication between different sites/clusters/pools that can leverage either asynchronous or synchronous

models so that various RPO SLAs can be achieved. The replication technology should be provided natively on the proposed platform.

- 1.1.23 For data protection roll back, the proposed technology should provide native integrated VM snapshots and enable configuration of automated VM snapshots backup via a user defined schedule.
- 1.1.24 The proposed solution must have the ability to cluster server-attached flash devices and/or mechanical disks, to provision a highly resilient shared datastore to support the hypervisor.
- 1.1.25 The proposed solution must be able to balance storage resources through automatic self-tuning and dynamic adjustment to workload storage demands.
- 1.1.26 The proposed solution must be able to improve storage efficiency through reclamation techniques with no compromise to availability and performance.
- 1.1.27 The proposed solution shall have native compatibility to integrate with Veeam Backup as an entire cluster for backup purposes.
- 1.1.28 The proposed solution shall have the ability to move/clone VMs across clusters (Prod, DR, UAT)

1.2 Micro segmentation

- 1.2.1 The proposed solution must be able to create a distributed firewall that gives administrators an application-centric policy management tool for securing Virtual Machine (VM) traffic.
- 1.2.2 The proposed solution must provide application centric firewall policies for VMs based on Application Topology (Independent of Physical Infrastructure, VLANs or Subnets).
- 1.2.3 The proposed solution must allow the adding VM(s) into firewall policy group and automatic inherit firewall policy.
- 1.2.4 The proposed solution must allow the movement of VM(s) between nodes without the need to reconfigure firewall policies.
- 1.2.5 The proposed solution must have the ability to securely isolate, quarantine and/or encapsulate all virtual machine instances.
- 1.2.6 The proposed solution must support user defined network security policy on an individual virtual machine basis.
- 1.2.7 The proposed solution must support Application Partitioning and isolation features.

1.3 Manageability

- 1.3.1 The proposed solution shall support scaling of management plane as the number of environments expand.
- 1.3.2 Integrated management console, for managing VM software and hypervisor upgrade on hyperconverged servers, should be provided without dependency on JAVA or Flash based technology leveraging on HTML5.
- 1.3.3 The proposed solution shall support centralised role-based governance.
- 1.3.4 The proposed solution must include AD-Integration for user authentication and access control.
- 1.3.5 The proposed solution shall monitor the health status of the entire solution and send out alerts for any abnormalities detected through SMTP.
- 1.3.6 The proposed solution must support license portability across server vendors.
- 1.3.7 The proposed solution shall include reporting features inclusive of but not limited to: Cluster Performance, Capacity Utilization, Space Reclamation.
- 1.3.8 The proposed solution shall include features that achieve VM-VM, VM-Host affinity.
- 1.3.9 The proposed solution shall include load balancing capabilities on the Host/Node and rebalance VMs automatically without disruption.
- 1.3.10 The proposed solution shall support audit logs to be forwarded to syslog or SIEM provider.

1.4 Availability Requirements

- 1.4.1 The proposed solution shall support native replication capability (RPO <= 4 hrs).
- 1.4.2 Virtualised storage controllers to instantly failover active I/O during upgrades with no VM down time.
- 1.4.3 The proposed solution shall support non-disruptive scaling by addition of nodes or tech refresh of nodes.
- 1.4.4 The proposed solution shall support non-disruptive removal of nodes.
- 1.4.5 The proposed solution shall natively support automatic failover of VMs in the event of a node failure without human intervention.

1.5 Resiliency Requirements

- 1.5.1 The proposed solution shall provide the capability to withstand, i.e. no degradation of compute effectiveness, the failure of one (1) node or one (1) disk in different blocks at the same time for production cluster.
- 1.5.2 The proposed solution shall provide the capability to withstand, i.e. no degradation of compute effectiveness, the failure of one (1) node or one (1) disk in different blocks at the same time for disaster recovery cluster.
- 1.5.3 A Single drive or node failure shall not result in an entire disk group failure.
- 1.5.4 The proposed solution shall maintain protection during drive or node failure, including during maintenance.
- 1.5.5 The proposed solution shall withstand failure of a single networking component such as Core Switch or Firewall in a high availability networking setup.
- 1.5.6 The proposed solution shall be self-healing where protection is started immediately without any delay during a disk or node failure. Self-healing shall be a fully automated process without the need for manual intervention and failure alerts shall be sent to support staff.
- 1.5.7 The proposed solution shall support predictive hardware failure by triggering a SMTP notification and/or displaying an alert via a Dashboard management console with constant monitoring of physical components including power supplies, fans, memory DIMMs and network adapters failure.

1.6 Network Switching Requirements

- 1.6.1 The proposed switch shall support a central management console.
- 1.6.2 The proposed switch must have advanced layer 2/3 feature set including VLAN, STP, LACP, QOS, BGP, OSPF, and VRF.
- 1.6.3 The proposed switch must have security features including Access Control Lists (ACLs) and port security.
- 1.6.4 The proposed switch must support dynamic segmentation.

1.7 Technical Requirements

1.7.1 The proposed Hyper-Converge servers and Virtualization Software shall conform to the requirements as specified in this Tender.

1.7.2 Supplier shall supply the Virtualization platform (Hardware + Software) for a single cluster of minimally **4** nodes for **Production site**:

The Production cluster shall have/at least:

- i. Total of 160 cores (Intel Xeon-Gold 6426Y 2.5GHz or higher) for the cluster.
- ii. Total of 5TB of Memory (4800MHz DDR5 RDM) for the cluster.
- iii. Total of 160TB effective storage capacity for the cluster.
- iv. Resiliency of 1 node with no impact/disruption to production workload (production workload defined as 96 cores, 3TB Memory, 100TB Storage capacity).

Each server in the cluster shall have/at least:

- i. 8 x 10Gb Network Interface (4 x VLAN to each server farm switch)
- ii. Required Network interface for Management VLAN

Software license subscription:

- i. Virtualization software licenses based on specifications of production cluster.
- ii. Central Management software licenses based on specifications of production cluster.
- iii. Micro-segmentation software licenses based on specifications of production cluster.
- iv. Disaster Recovery and replication software licenses based on 75 protected VMs.
- v. Management (Cluster performance and reporting) software license based on specifications of production cluster.
- vi. Any other software licenses required to meet the requirements specified.

1.7.3 Supplier shall supply the Virtualization platform (Hardware + Software) for a single cluster of minimally **2** nodes for **DR site**:

The Disaster Recovery cluster shall have/at least:

- i. Total of 96 cores (Intel Xeon-Gold 6426Y 2.5GHz or higher) for the cluster.
- ii. Total of 3TB of Memory (4800MHz DDR5 RDM) for the cluster.
- iii. Total of 100TB effective storage capacity for the cluster.
- iv. Resiliency of 1 node with no impact/disruption to DR workload (DR workload defined as 64 cores, 2TB Memory, 72TB Storage Capacity).

Each server in the cluster shall have/at least:

- i. 8 x 10Gb Network Interface (4 x VLAN to each server farm switch)
- ii. Required Network interface for Management VLAN

Software license subscription:

- i. Virtualization software licenses based on specifications of DR cluster.
- ii. Central Management software licenses based on specifications of DR cluster.
- iii. Any other software licenses required to meet the requirements specified.

1.7.4 Supplier shall ensure that hardware and software warranty come with 5 years and 24x7x4 Support.

1.7.5 Supplier shall ensure physical disk retention is included in the hardware maintenance.

1.7.6 Supplier shall take into consideration replication, snapshots, data-redundancy, deduplication, and any other factors when calculating effective storage capacity.

1.7.7 Supplier shall supply per **server farm switch** with at least **48-ports**:
Total quantity: **2** units at **Production site** and **2** units at **DR site**.

Each switch shall comprise these features and requirements:

- i. Switches with 10GbE (SFP/SFP+ and 10GBASE-T) and 40GbE populated as per required based on proposed server specifications.
- ii. Compatible transceiver module to be included for the link connection between server and server farm switches.
- iii. Compatible network cable for the link connection between server and server farm switches.
- iv. If proposed switches are not fully populated, supplier will be required to supply a total 15 x additional spare compatible transceiver module(ii) and compatible network cable(iii). If proposed switch is SFP-based, please cater for 10 sets for copper UTP connection, 5 sets for fibre connection.
- v. Existing connections to be migrated per switch:
 - a. 10GbE Fibre uplink to Firewall 1 (Cross-Rack)
 - b. 10GbE Fibre uplink to Firewall 2 (Cross-Rack)
 - c. 1GbE Copper UTP link to Replication Router (Cross-Rack)
- vi. Include software license required to deploy, connect, and troubleshoot an enterprise network, including:
 - a. Dynamic Segmentation
 - b. Switch Stacking
 - c. High Availability and Resiliency
 - d. Quality of Service (QoS)
 - e. Layer 2/3 Switching



- 1.7.8 Supplier shall supply C13/14 power cables for all proposed equipment for Production site (HQ).
- 1.7.9 Supplier shall supply UK power cables for all proposed equipment for DR site (IRC).
- 1.7.10 Supplier shall mount all proposed equipment within a single rack.

VENDOR'S EXPERIENCE IN SIMILAR PROJECTS

**** All requirement mentioned herewith are mandatory, sufficient details must be provided to demonstrate relevance to this project***

S/N	Item	Numbers / Description
1	Total number of successful relevant Server Infrastructure implementation projects in last 2 years with minimum project value of \$500k.	
2	Provide list of local client references of successful implementation of similar projects (at least 2 local client references)	
3	Provide client and project information of successful implementations of similar projects (at least 2 local client references) Client Information 1.1 Customer Name 1.2 Company Address 1.3 Company Description 1.4 Contact Person 1.5 Contact Person Telephone Number 1.6 Contact Person Email Address Project Information 1.7 2.1 Estimated Project Value (S\$) 1.8 2.2 Project / Scope Description 1.9 2.3 Duration of Project	

PROJECT REQUIREMENT

**All requirement mentioned herewith are mandatory*

S/N	Requirement	Comply (Yes / No)	Remarks
1	<u>Specifications</u> As specified in Functional requirements .		
2	<u>Specifications</u> As specified in Microsegmentation .		
3	<u>Specifications</u> As specified in Manageability .		
4	<u>Specifications</u> As specified in Availability requirements .		
5	<u>Specifications</u> As specified in Resiliency requirements .		
6	<u>Specifications</u> As specified in Network Switching requirements .		
7	<u>Specifications</u> As specified in Technical requirements .		
8	<u>Track Record</u> Please provide details listed in ANNEX C .		
9	<u>Value-Added Features</u> Please provide details listed in ANNEX E .		
10	<u>Bill of Materials (BoM)</u> Please provide a detailed BoM indicating all components included in the proposal.		
11	<u>OEM Undertaking Letter</u> Please provide OEM undertaking letter for each proposed hardware/software		
12	<u>Supporting Documents</u> Please provide supporting documents including but not limited to: proposed architecture (prod+dr), product features, effective compute and storage (including tabulation), proposed project timeline and schedule, project implementation plan, detailed information on VM conversion if required.		

Annex E**Valued-Added Features**

Please provide details on supported value-added features of proposed solutions not mentioned in the specifications and provide justifications on how the feature is achieved in the Justification column.

**You may list other relevant value-added features not mentioned in the list below.*

S/N	Features	Supported (Yes / No)	Justification
1	Management of solution is simplified		
2	Solution supports simplified hardware and software maintenance with zero downtime		
3	Solution supports near-zero RPO		
4	Solution supports native hybrid-cloud environment		
5	Solution is easily scalable		
6			
7			

POST-DEPLOYMENT SUPPORT

**Please indicate if the following describes the post deployment support services provided.*

S/N	Requirement	Supported (Yes / No)	Remarks
1	Single point of contact for support for all technologies.		
2	Support team is based locally in Singapore.		
3	Dedicated support resource will be assigned.		
4	Periodic health checks and performance review will be performed with advisory provided.		
5	Professionally certified engineers (Based on proposed solution)		