KENYATTA NATIONAL HOSPITAL

Address: P.O BOX 20723-00202, Nairobi.
Telephone: 020 2726300-4 | 020 4243000 | 020 7244000
Cellphone Numbers: 0730 643 000 | 0709 854 000 | Email: knhadmin@knh.or.ke

Ref: KNH/SCM/ADM.43 Date: 24th September, 2026

ADDENDUM

To: ALL BIDDERS

RE: ADDENDUM TO PREQUALIFICATION NO: KNH/T/72/2026-2027 SUPPLY, INSTALLATION, CONFIGURATION AND COMMISSIONING OF PERIMETER FIREWALL FOR KENYATTA NATIONAL HOSPITAL

Pursuant to the Public Procurement and Asset Disposal Act section 75 and its attendant Regulations 2020 and Clause 7 on Amendment of Tender Documents, the Hospital wishes to make the following amendments/clarifications;

1. **Technical Specifications for Perimeter Firewall has been EXPUNDGED and replaced with Annex 1 attached.**

Tender Opening and Closing date has been AMMENDED to read as **7th October, 2026. 10.00 hours Kenyan time.**

Dr. Abdallah Ofula
FOR: CHIEF EXECUTIVE OFFICER

ANNEX 1

KENYATTA NATIONAL HOSPITAL

Address: P.O BOX 20723-00202, Nairobi.
Telephone: 020 2726300-4 | 020 4243000 | 020 7244000
Cellphone Numbers: 0730 643 000 | 0709 854 000 | Email: knhadmin@knh.or.ke

INTERNAL MEMO

OFFICE OF THE HEAD OF DEPARTMENT, ICT

KENYATTA NATIONAL HOSPITAL RECEIVED 22 SEP 2026 DIRECTOR SUPPLY CHAIN MANAGEMENT P.O Box 20723 - 00202 NAIROBI

Ref: KNH/ICT/S&P/03/ (125)

To: Director, Supply Chain Management
KNH

Date: 22nd September 2026

RE: ADDENDUM TO THE REQUEST FOR PROCUREMENT OF FIREWALL LICENSES FOR FY 2026/2027

Attached herewith are the reviewed specifications for your consideration and appropriate action.

Lucas Ngoge
HoD , ICT

Cm/procurement)
Pls discuss with the specs
Asap
23/9/2026

TECHNICAL REQUIREMENTS/SPECIFICATIONS

At this stage, the evaluation shall determine whether the bidder is technically responsive to all the specified requirements. Bidders shall be required to submit detailed, highlighted technical specifications demonstrating compliance with the requirements, together with relevant manufacturers' catalogues and/or brochures for the equipment to be supplied.

S/No.	Item description	Technical Specifications	Bidder must Indicate the Name and Model of the proposed solution /component
1.	Perimeter Machine Learning Powered NGFW	Hardware Appliance - Including licenses and support for 1yr	
2.	Centralized Management	Hardware Appliance – Including license and support for 1yr	
3.	Operation	The NGFW platform must not experience performance degradation when all security features turned on. The solution should utilize hardware acceleration (SecureXL) and multi-core CPU parallel distribution (CoreXL) to execute Stateful Inspection, Application Control, and Threat Prevention in a single traffic flow.	
		The NGFW should support Decryption for TLSv1.3	
		Visibility into applications using non-standard ports	
		Must support App-ID, User-ID and Content-ID without additional license. Out of box provisioning.	
		Should support ISP load balancing using ECMP	
4.	Performance	Advanced Threat prevention throughput of 6.5Gbps (Threat Prevention must be measured with Application Awareness, Intrusion Prevention, Antivirus, Sandboxing, URL Filtering, File Blocking, Antivirus and full logging enabled simultaneously)	
		Firewall Throughput 55 Gbps	
		IPsec VPN Throughput 22.1 Gbps	
		Virtual systems Supports up to 25+ Virtual Routers/Systems	
		New Connections/Sec: 190,000	

		Concurrent Connections: Up to 16.2 Million max	
5.	Interfaces	**10 x On-board 10/100/1000/10000 Base-T RJ45** Management & Sync ports.	
		Expansion Slot Card Options: 8 x 1/10GbE SFP+ or 4 x 10/25GbE SFP28	
6.	Advanced Theft Prevention	Utilizes 70+ AI/ML engines feeding real-time global telemetry into the gateway for zero-day variant detection.	
		Inline detection system to prevent unknown and evasive C2 threats, including those produced through the Empire framework, as well as command injection and SQL injection vulnerabilities.	
		Virtual patching and behavioral vulnerability shielding against unknown injection vectors.	
		Runs quick local heuristic/ML checks on-box for immediate verdict delivery before sandboxing.	
		Dynamic risk scoring and automated false-positive suppression via global AI evaluation.	
7.	Advanced URL Filtering	AI models continuously analyze domain reputation and DNS queries.	
		In-line cloud lookups evaluate un-categorized URLs in real-time.	
		Multilayer database categorized by dynamic web crawlers, AI classifiers, and human analysis.	
		Blocks corporate credential submission on deceptive, look-alike, or non-corporate sites in real time without browser extensions.	
		Analyzes page layout, logos, fonts, and DOM elements in real-time to detect visual brand impersonation.	
		Global language crawling support for international domains and non-English phishing campaigns.	
8.	Advanced Sandbox	AI-driven CPU-level sandboxing that detects evasive malware before execution.	
		File structural analysis combining custom YARA rules, dynamic signature extraction, and ML scoring.	
		Detonates files in isolated sandbox environments, tracking system-call hooks, registry modifications, recursive process spawns, and outbound C2 calls.	
		Full inspection support for Windows PE, macOS binaries, ELF, Android APKs, Office documents,	

		PDFs, archives (ZIP/RAR/7z), scripts (JS/VBS/PS1/Shell), and encrypted attachments.	
		Full API access allowing external security tools (SIEM/SOAR) to submit files to Threat Emulation and retrieve sandbox analysis reports.	
9.	Advanced DNS Security	Domain Generation Algorithms (DGA), DNS tunneling and Command & control (C2) detection made capable by machine learning, enabling Identification of threats hidden within DNS traffic	
		Algorithmic calculation of domain randomness and entropy scoring.	
		Instant inline drop of requests destined for algorithmic C2 domains.	
		Redirects rogue DNS queries from compromised internal hosts to an isolated gateway IP for remediation.	
		DNS tunnel detection detects payload steganography and high-frequency TXT/NULL record queries used for data exfiltration.	
		Automated active drop and host isolation upon detecting DNS-based data exfiltration.	
		Continuous cloud updates for new malicious domains and DNS IOCs.	
		Layered architecture operating beyond traditional URL/domain reputation filtering.	
10.	Required Licenses	Advanced Threat Prevention	
		Advanced URL Filtering	
		Advanced DNS Security	
		Advanced SD-WAN	
11.	Manufacturer Authorization	Manufacturer's letter Authorization (As Per Sample Specified in tender document)	
12.	Supporting Documents	Technical literature/brochure supporting the supplied product	
13.	Warranty	1 Year proactive & onsite Warranty from Original Equipment Manufacturer (OEM).	
14.	Deployment	Provide Statement of Works (SoW) that shows how the OEM will deploy the solution	
15.	Centralized Management - Interfaces	Should have 2 100/1000/10000 mbps interface	

16.	Centralized Management -Storage	6 x 4 TB Enterprise HDDs configured in RAID-5/10 (yielding ~16 TB–20 TB usable log storage).	
		Expandable up to 24 TB raw/usable RAID enterprise storage.	
17.	Centralized Management -Server	Dual 750W Hot-Swappable Redundant Power Supplies.	
		Auto-switching 100–240 VAC (50–60 Hz).	
		Rated up to 10A @ 100-120 VAC.	
		Enterprise hardware platform designed for high MTBF standards with redundancy across power and storage.	
18.	Centralized Management - License	Support management of 25 devices with the base license	
19.	Deployment Service	Professional deployment service from OEM. -Include Statement of Work (SoW)	
20.	Training	Training of 3 Delegates by OEM Trainer to cover all solutions	
21.	Manufacturer Authorization Form(MAF)	MAF signed by OEM	

NB; the vendor must deliver, install, configure, test, commission, and provide comprehensive training on the supplied solution.

TECHNICAL EVALUATION – VENDOR CAPACITY

No	ITEM	Description	
1	Compliance	Compliance to all the technical specifications/ Mandatory technical compliance section	10 Marks
2	Bidders Experience	I. Bidder should provide three (3No) clients where they have undertaken/provided ICT security solution within the last 6 years (2019-2025). The three projects should be of a minimum combined value of Kes 100M and above. (2marks for each clients)	6 Marks
		II. Attach evidence in form of a copy of contract/LPO or a completion certificate, all should be certified by Commissioner of oaths/advocate and provide the list of the organizations, contact person and value of the project for sites mentioned above. (5marks for each Contract/LPO & Completion certificate)	15 Marks
		III. Bidder must provide 1 (one) reference site for a Network Access control contract from a large institution. The project must include implementation and support (SLA). Attach evidence in form of a copy of contract/LPO or a completion certificate certified by Commissioner of oaths/advocate.	6 Marks
3	Key Personnel Resources	The installation of the solutions SHALL be performed by a certified team of ICT professionals. As detailed below (Attach Proof)	
		Demonstrate that your firm has human resource capacity to successfully deliver the project. To demonstrate this, bidders should submit details of key personnel that will undertake the implementation of project at all stages (design, installation, training, and maintenance) and their availability for the duration of the project.	4 Marks
		Project Lead Engineer:	
		One (1) Project Lead with an ICT related degree and more than eight	10 Marks

		(8) years relevant work experience in implementing and administering Cyber Security tools, IT Networks, and knowledge of the various Operating Systems; and IT system Support and maintenance. Demonstrate competency in the implementation and administration of various security tools e.g. Firewalls and NAC's. The Project Lead Engineer MUST have professional certification i.e. CCNP Enterprise, Cisco Certified Specialist – Network Security Firepower, Cisco Certified Specialist – Security Core, CCSE or any related professional vender proof certification.	
		Enterprise Network Engineers:	
		One (1) Enterprise Network Engineer with an ICT degree and more than five (5) years of relevant work experience in design installation and maintenance of network and cyber-security infrastructure solution. The Network engineer MUST have Network professional certification. E.g., CCNP Enterprise, CCNP Security, CCSE or any related professional vender proof certification.	5 Marks
		Technical Implementation Engineers:	
		At least Three (3) Technical Engineers with an ICT related degree and more than Three (3) years of relevant experience Telecommunication/ICT field especially in ICT security functional area The three technical Staff MUST have associate certifications in Network Technology: HCNA, CCNA, ACE 5, HCIA or any related professional vender proof certification. (3marks for each engineer)	9 Marks
		Project Management Staff:	
		One (1) Project Management professional and more than Five (5) years of experience. MUST have a PhD or master's degree in Information Security and Audit CAPM, PMP, Prince II certification or Agile Certifications The qualification SHALL be verified to establish authenticity (Attach certified certificate & CV of each engineer/staff mentioned above, signed by the employee and the director. Due diligence	5 Marks

		confirmation will be carried out including online verification and background checks).	
4	Letter of undertaking	A written undertaking signed by the firm confirming availability of the staff mentioned above to carry out the assignment upon winning the bid. The written undertaking shall be addressed to CEO, Kenyatta National Hospital and must be specific to this tender	5 Marks
5	Draft SLA	Draft Service Level Agreement detailing: 1. Fault Logging procedures 2. Severity Level & priority definition. 3. Service level definition indicating response timelines & coverage. 4. Escalation Matrix 5. Reactive Maintenance activities and scope 6. Preventative Maintenance activities and scope 7. Proactive monitoring activities and scope (2 Marks each detail mentioned above)	10 Marks
6	Project Implementation	Provide project implementation methodology and workplan in form of a Gantt Chart detailing activities, milestones and timelines for each milestone. Adequacy of the proposed methodology and work plan as follows: 1. Proposed preventive maintenance sub-plan 2. Proposed corrective maintenance sub-plan 3. Proposed test and quality assurance sub-plan 4. The bidder should provide a draft Service Level Maintenance SLA (5 Marks each detail mentioned above)	15 Marks
	Total Marks		100