

13. ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް

13.1 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް 1 ގެ ޕްލާން ގައި ސަބަބު ޖެނެރަލް ޕްރޮސެކިއުޓަރ (ޖެނެރަލް ޕްރޮސެކިއުޓަރ)

13.2 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

13.3 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

13.4 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

13.5 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

13.6 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް

13.7 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

13.8 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

13.9 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

13.10 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް

13.11 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި 500,000/- (ފަންސަވަރު) ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި 0.05% ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

13.12 ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި ޖެނެރަލް ޕްރޮސެކިއުޓަރ ގެ އޮފީސް ގައި

Annex 1

Bid Submission Form

Iulaan No: (IUL)94-Q/94/2022/28

IMPORTANT: This sheet should serve as a front page of the proposal. If any bidder fails to submit the relevant information and bid documents states in information sheet section 14, bid will be rejected at the bid opening stage.

Bid Title: Sophos End point Security for 12months Subscription

Qty	Description	Price
200	Central Intercept x Endpoint Advanced – COMP UPG	
25	Central Intercept X Advanced for Server (previously Central Server Protection Advanced)	
GST (6%)		
TOTAL (MVR)		
Total in Words:		

Delivery	Calendar days	
Proposed Delivery Period		days

Check list for documents submitted (please tick the appropriate box)

		Yes (✓)	No (x)
1	Bid Submission Form Completed & Signed		
2	Certificate of Registration (Company)		
3	Memorandum of Association (for companies)		
4	National Identity Card		
5	Certificate of Registration (Sole Proprietorship)		
6	Company Profile		
7	S.M.E Registration		
8	G.S.T Registration		
9	Past Experience Documents (Related to the bid)		
10	Tax Clearance Form		
11	Bid Security (If the bid amount is greater than 500,000.00)		
12	Bank Statement		

Annex 02

Technical Requirement

SL. No.	Technical Specifications for Server security	Compliant / Non Compliant
1	The antivirus solution should provide enhanced dedicated antivirus protection for servers of all the attacks originating from places inside/outside of the network due to virus and/or other malicious programming code.	
2	The antivirus solution Should have a Centralized Management Console with off-premise model.	
3	The vendor must have its own proprietary scan engine	
4	The antivirus solution Should Support Multi-Platform operating system (Windows,Linux) and the same should be managed from a single Centralised Management cosole	
5	The antivirus solution Should have single, Configurable Installation with centralized configuration & policy management.	
6	Antivirus should support integration with Active directory for directory structure of computers for better management	
7	Solution must Prevent update storms and Scan Storms for virtualised environment	
8	Solution must have virtualization support vsphere & Hyper V	
9	Solution must have off-board malware protection to a centralised security virtual machine	
10	Solution must have the File Integrity Monitoring module for windows server 2008 R2 & above.	
11	Solution must offer default monitored locations for File integrity monitoring for Files/registry entries for Windows server 2008 R2 platforms	
12	Solution should have feature of Monitoring events & storing on a local server with option to send them to the Windows Event Viewer	
13	Solution must support Malicious Traffic Detection to monitor non-browser-based traffic for any Command & Control (C&C) Servers connection.	
14	Administrator should have flexibility to schedule Scan and update Antivirus Agents from central Server.	
15	Solution should have the feature in which user activity is logged and viewable directly within management Console for, allowing administrators to audit and identify undesirable behavior	
16	Antivirus should be able to capture Viruses, Trojans, Worms, Spyware and Malware, Adware and PUA from single agent.	

17	Solution should have Data control that enables you to monitor and control the transfer of files from computers to storage devices and applications connected to the internet.	
18	Solution should support Data Protection Policy to monitor data copied or shared through external mediums and internet browsers.	
19	Anti-Virus Should have Host Intrusion Prevention System (HIPS) technology which works in 4 Layers to provide zero-day protection without the need for updates (Unknown Virus Detection & Repair),	
20	Anti-Virus Software must have the capability to clean, Quarantine or delete Viruses and should be able to detect new classes of viruses by normal virus definition update mechanisms	
21	Solution should have use pre-execution analysis to detect threats without letting the code run, avoiding the risk of partial infection and damage	
22	Administrator Should be able to add files, folders or extensions to an exclude list so that they are not scanned on access.	
23	Should enable automatic submissions of unknown/suspected virus samples to vendor and automatic response/delivery of the cure.	
24	Administrator should be able to lock down all anti-virus configurations at the server & User should be prevented from being able to uninstall the anti-virus software.	
25	Solution must have the Server Lockdown facility to lock the state of server to protect its integrity.	
26	Antivirus should provide centralized event logging to locate and cure virus problems.	
27	Solution must protect against ransomware running locally or remotely	
28	Alerts on virus activity should be passed on to administrator	
29	Solution should have Live protection with Web Reputation	
30	Solution Application control should also have the capability to restrict the usage and block the applications even if they are installed on category basis ie. Whitelisting & Blacklisting of the applications	
31	Antivirus solution should have integrated Data Loss Prevention module with pre-defined templates.	
32	Antivirus solution should have integrated DEVICE control module with a feature to set devices to "Read Only", "Add Exceptions" and " Block" Black listing and whitelisting of the devices.	
33	USB mass storage device Blocking and Exceptions with Vendor and Model (Device ID)	
34	Integrated HIPS for Easy of Management and Protection	

35	Solution must have capability to Stop real-world hacking techniques like but not limited to Credential harvesting Lateral movement Privilege escalation	
36	OEM Should have 24x7x365 toll free Global Technical Support	
37	Solution must have the privilege to log a support case from the management dashboard	
38	Proposed Solution should be in 'Leaders' quadrant of the gartners Magic Quadrant for Endpoint protection platform in the recent year.	
39	Solution must have the Anti exploit technology on signature less basis so that it protects against browser, plugin, or Java-based exploit kits even if your servers are not fully patched	
40	solution must be powered by Deep Learning Neural Network	
41	Solution must have the Threat cases that generate Root Cause Analysis that provides the who, what, when, where, and how of a given attack, allowing IT the ability to constantly improve upon their security posture	
42	Solution must automatically identify and stops unwanted encryption attempts as well as system-crippling MBR attacks	
43	Solution must have Anti-Hacker Capabilities that protects against the most persistent hacking attempts and prevents pervasive, real-time hacking techniques such as credential harvesting, lateral movement, and code-caving	
44	Solution should be capable to discover and Ensure AWS and Azure Workloads are Protected and Compliant	
45	Solution should be able to create sub tenants as required	
46	Solution should be able to create roles eg: Admin, Super admin, helpdesk etc	
47	Solution should be capable of XDR ready if license permits	
48	Solution should support below two factor authentication methods Email security code with pin code SMS Google Authentication APP	

