

GSR – KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT

Centralized Endpoint Security, Offline Client Update & DMZ-Based Update Server

AFIC requires Kaspersky Endpoint Security for Business SELECT (or an equivalent enterprise endpoint security solution) for approximately 200 client endpoints. The proposed solution shall provide centralized endpoint protection and management, with a dedicated update server deployed in the AFIC DMZ. The primary objective is to ensure that client endpoints do not connect directly to the Internet for security updates or other update related communication.

The detailed specifications and terms and conditions are as follows:-

Both soft copies as well as hard copies of specified documents are required.

Submit all documents in soft copy to: gso2it@afic.gov.pk

Submit all documents in hard copy also to the address: IT Department, main AFIC building, AFIC, Rawalpindi.

Last date of Bid submission: 18 Sep 2026

Ser	Eqpt	Qty	Specs	Remarks
1.	KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT OR EQUIVALENT	200	Enterprise endpoint security licenses for 200 client endpoints. Centralized endpoint protection and management.	
			Protection against malware, viruses, ransomware and other supported endpoint threats.	
			Centralized endpoint policies and device control, endpoint status, update status, threat events and reporting.	
2.	KASPERSKY UPDATE / MANAGEMENT SERVER	1	Dedicated server-based update/management solution to be deployed in AFIC DMZ. Server shall obtain required Kaspersky updates online through controlled Internet access.	
			Secure/hardened DMZ deployment; scheduled synchronization; controlled client distribution; bandwidth optimization.	
3.	DMZ UPDATE ARCHITECTURE	1	Internal client endpoints shall not have direct Internet connectivity for Kaspersky updates. Client endpoints shall receive updates from the centrally deployed internal/DMZ update infrastructure in an offline/controlled update model (the organization requires 1 x instance of management server within DMZ for regular updates and a mechanism for downloading these updates and ingesting them in internal management server through air gap).	
4.	CENTRALIZED MANAGEMENT	1	Centralized console for endpoint administration, security policies, monitoring, alerts and reporting for approximately 200 clients.	
5.	UPDATE MANAGEMENT	1	Scheduled synchronization/download of Kaspersky database/product updates on the DMZ server and controlled distribution to clients.	

6.	NETWORK & SECURITY CONFIGURATION	1	Firewall controlled communication between Internet, DMZ and internal clients. Bidder shall specify required ports, protocols, URLs/domains and security requirements.	
----	----------------------------------	---	---	--

7.	IMPLEMENTATION & CONFIGURATION	1	Complete turnkey installation, end-to-end configuration, policy creation and deployment assistance for 200 clients.	
			Testing and commissioning of update synchronization, client update process and direct Internet restriction.	
			As built architecture, communication flow, ports, firewall rules and administrator documentation.	

8.	ANNUAL SUPPORT SERVICES	1	Minimum 1 x year online & onsite & remote technical support, troubleshooting and escalation.	
			Preventive health check, update assistance, service response time and escalation matrix.	
9.	PROFESSIONAL TRAINING	1	Professional administrator training for nominated AFIC IT staff covering administration, policies, updates, monitoring, reporting and troubleshooting.	

Acceptance Criteria	1 x year support services to include: Online Support; Service level response time; Preventive Maintenance/health check; on site troubleshooting; Software/update assistance; if any.	
	Successful bidder shall provide demo/technical evaluation, turnkey installation, end to end configuration and integration with AFIC client endpoints. Required server software, network/security configuration and firewall requirements shall be included. Bidder shall specify all extra/allied equipment or software. Compliance sheet against every GSR feature is compulsory. Facility survey may be requested before finalizing design.	
Quotation Submission Requirements	All bidders are required to compulsorily submit supporting documents with their bids (list attached as Anx-A). Any document missing will render the bidder unqualified. Firms will be subjected to technical scrutiny of the solution, architecture and design offered. Technically qualifying firms will be subjected to financial shortlisting based on financial bids submitted.	
Quotation Submission Requirements	All bidders are required to compulsorily submit supporting documents with their bids (list attached as Anx-A). Any document missing will render the bidder unqualified. The bidding firms will be subjected to technical scrutiny of the equipment, design offered. Firms qualifying technically will be subjected to financial shortlisting basing on the financial bids submitted.	

Anx- A**List of Supporting Documents**

Ser	Supporting Document
1.	Equipment/Software/Services offered along with price as per format given at Anx-B
2.	Compliance sheet as per Anx-C

Anx- B**Equipment Offered with Price**

Ser	Equipment/ Services	Specifications	Price
1.	Kaspersky Endpoint Security for Business SELECT OR EQUIVALENT	200 Client Licenses	
2.	DMZ Update / Management Server & Implementation	1 Set turnkey deployment, configuration and integration	
3.	Annual Support & Professional Training	1 Year Support + Administrator Training	Total price:

Anx- C**Compliance Sheet Format**

Ser	Eqpt	Qty	Specs	Fully compliant/ partially compliant/ non compliant
1.	KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT OR EQUIVALENT	200	Enterprise endpoint security licenses for 200 client endpoints. Centralized endpoint protection and management.	
			Protection against malware, viruses, ransomware and other supported endpoint threats.	
			Centralized endpoint policies and device control, endpoint status, update status, threat events and reporting.	
2.	KASPERSKY UPDATE / MANAGEMENT SERVER	1	Dedicated server-based update/management solution to be deployed in AFIC DMZ. Server shall obtain required Kaspersky updates online through controlled Internet access.	
			Secure/hardened DMZ deployment; scheduled synchronization; controlled client distribution; bandwidth optimization.	
3.	DMZ UPDATE ARCHITECTURE	1	Internal client endpoints shall not have direct Internet connectivity for Kaspersky updates.	

			Client endpoints shall receive updates from the centrally deployed internal/DMZ update infrastructure in an offline/controlled update model (the organization requires 1 x instance of management server within DMZ for regular updates and a mechanism for downloading these updates and ingesting them in internal management server through air gap).	
4.	CENTRALIZED MANAGEMENT	1	Centralized console for endpoint administration, security policies, monitoring, alerts and reporting for approximately 200 clients.	
5.	UPDATE MANAGEMENT	1	Scheduled synchronization/download of Kaspersky database/product updates on the DMZ server and controlled distribution to clients.	
6.	NETWORK & SECURITY CONFIGURATION	1	Firewall controlled communication between Internet, DMZ and internal clients. Bidder shall specify required ports, protocols, URLs/domains and security requirements.	

7.	IMPLEMENTATION & CONFIGURATION	1	Complete turnkey installation, end-to-end configuration, policy creation and deployment assistance for 200 clients.	
			Testing and commissioning of update synchronization, client update process and direct Internet restriction.	
			As built architecture, communication flow, ports, firewall rules and administrator documentation.	

8.	ANNUAL SUPPORT SERVICES	1	Minimum 1 x year online & onsite & remote technical support, troubleshooting and escalation.	
			Preventive health check, update assistance, service response time and escalation matrix.	
9.	PROFESSIONAL TRAINING	1	Professional administrator training for nominated AFIC IT staff covering administration, policies, updates, monitoring, reporting and troubleshooting.	