SỞ Y TẾ
THÀNH PHỐ HỒ CHÍ MINH
BỆNH VIỆN MẮT

Số: 1902 /BVM-HCQT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Thành phố Hồ Chí Minh, ngày 21 tháng 11 năm 2025

YÊU CẦU MỜI CHÀO GIÁ

Áp dụng đối với gói thầu "Mua sắm phần mềm diệt virus cho các Khoa, Phòng"

Kính gửi: Các Doanh nghiệp, nhà cung cấp, hộ kinh doanh quan tâm.

Bệnh viện Mắt có nhu cầu tiếp nhận chào giá để tham khảo, xây dựng giá gói thầu "Mua sắm phần mềm diệt virus cho các Khoa, Phòng" với nội dung cụ thể như sau:

I. Thông tin của đơn vị yêu cầu chào giá:

1. Đơn vị yêu cầu mời chào giá: Bệnh viện Mắt.

2. Mã số thuế: 0301483745

3. Địa chỉ: Số 280 Điện Biên Phủ, Phường Xuân Hòa, Thành phố Hồ Chí Minh.

4. Điện thoại: 028 39 325 364.

5. Cách thức tiếp nhận tài liệu chào giá: Nhận trực tiếp qua đường văn thư tại địa chỉ: Phòng Hành chính quản trị - Bệnh viện Mắt – Địa chỉ: 280 Điện Biên Phủ, Phường Xuân Hòa, Thành phố Hồ Chí Minh.

Trên phong bì ghi rõ:

Tiêu đề: "Chào giá gói thầu "Mua sắm phần mềm diệt virus cho các Khoa, Phòng" theo công văn mời chào giá số 1902/BVM-HCQT"

Nơi nhận: Bộ phận tiếp nhận văn thư đến phòng Hành chính quản trị - Bệnh viện Mắt – 280 Điện Biên Phủ, Phường Xuân Hòa, Thành phố Hồ Chí Minh.

6. Thời hạn tiếp nhận chào giá: Hạn chót đến 16 giờ ngày 05 tháng 12 năm 2025.

7. Thời hạn có hiệu lực của chào giá: Tối thiểu 30 ngày, từ ngày phát hành chào giá.

II. Danh mục yêu cầu mời chào giá:

1. Danh mục số lượng mời chào giá:

STT	TÊN DANH MỤC	ĐƠN VỊ TÍNH	SỐ LƯỢNG	GHI CHÚ
01	Phần mềm diệt virus dành cho máy tính và máy chủ	Bộ/ bản quyền/ license	526	520 máy tính và 6 máy chủ

1.1. Danh mục số lượng máy chủ

STT	Tên máy chủ	Số lượng
01	Máy chủ dành cho phần mềm kế toán	01
02	Máy chủ dành cho phần mềm xét nghiệm (LIS)	01
03	Máy chủ dành cho phần mềm quản lý bệnh viện (HIS)	01
04	Máy chủ dành cho các phần mềm khác	01
05	Máy chủ dành cho backup dữ liệu HIS	01

06	Máy chủ dành cho phần mềm HFS	01
	Tổng cộng:	**06**

1.2. Danh mục số lượng máy tính, laptop, kiosk Khoa, Phòng

STT	Tên khoa phòng	Máy tính	Laptop	KIOSK
01	Phòng Kế hoạch Tổng hợp;	19		
02	Phòng Chỉ đạo tuyến;	7		
03	Phòng Tổ chức Cán bộ;	15		
04	Phòng Tài chính Kế toán;	35		
05	Phòng Hành chính Quản trị;	14		
06	Phòng Điều dưỡng;	3		
07	Phòng Vật tư - Thiết bị y tế;	24		
08	Phòng Công nghệ Thông tin;	22	4	
09	Phòng Quản lý Chất lượng;	7		1
10	Phòng Công tác xã hội;	19		3
11	Khoa Giác mạc;	15		
12	Khoa Glaucoma;	18		1
13	Khoa Dịch kính võng mạc;	25		1
14	Khoa Mắt nhi;	14		
15	Khoa Khúc xạ;	35		
16	Khoa THTM - TKNK;	12		
17	Khoa Tổng hợp;	21		
18	Khoa Khám mắt;	73		
19	Khoa Phẫu thuật gây mê hồi sức;	32		
20	Khoa Dinh dưỡng;	2		
21	Khoa Cấp cứu;	20		
22	Khoa Dược;	39		
23	Khoa Xét nghiệm;	15		1
24	Khoa Chẩn đoán hình ảnh;	18		
25	Khoa Kiểm soát nhiễm khuẩn.	5		
		509	**4**	**7**
	Tổng cộng	**520**		

2. *Địa điểm thực hiện:*

+ Cơ sở 1: 280 Điện Biên Phủ, Phường Xuân Hòa, Thành phố Hồ Chí Minh

3. *Thời gian thực hiện:* 90 ngày

4. *Danh mục thông số và yêu cầu kỹ thuật chi tiết:*

STT	Tên danh mục	Yêu cầu kỹ thuật
01	Phần mềm diệt virus dành cho máy tính và máy chủ	**1/ Yêu cầu chung** Quản trị tập trung. Bảo vệ máy trạm, máy chủ và hệ thống ảo hóa trước các nguy cơ về virus, ransomware, tấn công mạng, kiểm soát thiết bị, kiểm soát web.

		Quản trị tập trung qua web console. **2/ Tính năng** **Tính năng Anti-Virus** Sản phẩm có tên trong các lần công bố danh mục sản phẩm phòng, chống phần mềm độc hại đáp ứng yêu cầu kỹ thuật theo Chỉ thị số 14/CT-TTg ngày 25/5/2018. Ngôn ngữ phần mềm: hỗ trợ tiếng Việt và tiếng Anh **Triển khai trên các hệ điều hành:** Máy trạm và máy chủ: Windows, Linux, Mac Thiết bị di động: Android, IOS **Khả năng bảo vệ** **Khả năng bảo vệ chống Malware** Có khả năng phát hiện và diệt viruses, spyware, worm, trojan rootkit, keyloger macro,… Cho phép lựa chọn quét nhanh, quét full, quét tức thời, quét theo lịch trình và hỗ trợ quét từ xa qua giao diện quản lý tập trung. Giải pháp hỗ trợ quét thời gian thực các file truy xuất. Có khả năng chỉ quét những file mới và những file có sự thay đổi so với lần quét virus gần nhất giúp tăng tốc độ quét virus. Giải pháp phải quét bộ nhớ hệ thống để phát hiện các rootkit, tiến trình ẩn, và các hành vi khác cho thấy mã độc hại đang cố gắng ẩn giấu. Giải pháp có chức năng bảo vệ Web, đáp ứng quét cho traffic web, email, file theo cơ chế chủ động. Giải pháp đáp ứng chức năng thông báo cho người sử dụng và quản trị hệ thống về việc phát hiện đối tượng bị nhiễm mã độc qua hộp thoại cảnh báo cho người sử dụng; Email và gửi tới SIEM cho người quản trị. Cho phép người quản trị có thể thiết lập mặc định các hành động sẽ thực hiện khi chương trình phát hiện mã độc: alert/ notify, clean, delete/remove, move/quarantine. Hỗ trợ các tính năng mà nhờ đó người quản trị có thể lập kế hoạch ngăn chặn việc bùng nổ lây lan virus trong hệ thống. Bảo vệ các nguy cơ từ Email bằng việc quét toàn bộ các Email vào/ra để phát hiện và ngăn chặn các nguy cơ từ Email. Hỗ trợ các giao thức: POP3, SMTP, IMAP Ngăn chặn xâm nhập vào máy chủ ngăn chặn các ứng dụng thực hiện các hành vi nguy hiểm cho hệ điều hành đảm bảo quyền truy vào tài nguyên hệ điều hành và dữ liệu cá nhân **Chức năng giám sát mạng và giám sát hệ thống** Cho phép xem toàn bộ các kết nối mạng trên máy tính theo thời gian thực. Cho phép ghi lại hoạt động của các ứng dụng trên máy tính, cung cấp thông tin này để nâng cao tính bảo mật. **Chức năng tường lửa** Phải có chức năng hỗ trợ kiểm soát traffic vào/ra. Cho phép thao tác kiểm soát Firewall Client từ xa như: Disable,

		Enable từ xa. Giải pháp phải có khả năng cảnh báo, giám sát các ứng dụng đang chạy. Cho phép tạo ra tập luật (rule) dựa trên ứng dụng hoặc mạng (application network, network packet rule). Hỗ trợ các dạng protocol: TCP, UDP, ICMP, IGMP. **Chức năng Device control** Phải có khả năng ngăn chặn thiết bị nào có thể hoặc không thể sử dụng trên Windows. Phải có khả năng ngăn cấm các ứng dụng chạy từ thiết bị lưu trữ ngoài. Phải có khả năng thiết lập lịch được sử dụng thiết bị cắm ngoài qua giao tiếp USB. Cho phép thiết lập danh sách các thiết bị cắm ngoài được sử dụng (Trusted Device). **Chức năng Web Control** Lọc web theo URL, category, data, content. Giới hạn truy cập Web theo lịch - Cho phép quét toàn bộ giao tiếp thông qua giao thức HTTP, HTTPS, kiểm tra toàn bộ URL xem có trong danh sách các website chứa mã độc hay website lừa đảo hay không. - Cho phép tạo ra các luật để hạn chế hay cấm người dùng truy cập vào những nội dung không cho phép. - Tập luật có thể thực hiện theo lịch, cho phép các luật thực hiện theo thời gian cụ thể. **Chức năng Application Control** Cho phép thiết lập danh sách trắng bằng việc phân loại các ứng dụng theo đánh giá của nhà sản xuất, hoặc sử dụng công nghệ điện toán đám mây. Cho phép tạo ra danh sách trắng các ứng dụng theo nhóm người sử dụng bằng việc kết hợp với AD/LDAP. Khả năng thiết lập danh sách đen các ứng dụng theo nhóm, theo sự phân loại của nhà sản xuất hoặc theo cơ chế bảo mật của mỗi đơn vị sử dụng. **Chức năng Virus Update** Hỗ trợ cập nhật bằng tay tại Client từ Server quản lý. Hỗ trợ cập nhật cho nhiều Client từ Server quản lý. Hỗ trợ lập lịch tự động download update. Server quản lý trung gian: Có thể tải cập nhật từ nhiều nguồn khác nhau (từ server quản lý cấp trên, từ nhà cung cấp qua Internet), có thể thiết lập việc lựa chọn nguồn update. Giao thức dùng để cập nhật virus từ nhà cung cấp, từ máy chủ là giao thức chuẩn: HTTP,HTTPS, FTP, SMB share và có thể hoạt động thông qua Proxy. **Chức năng quét lỗ hổng bảo mật** Có khả năng quét lỗ hổng bảo mật các sản phẩm của Microsoft và các hãng khác. Bảo vệ thiết bị khỏi ransomware bao gồm cả các thư mục chia

		sẻ trên máy chủ. **Một số chức năng bảo vệ khác** Thành phần bảo vệ AMSI hỗ trợ quét phần mềm độc hại từ Microsoft **Khả năng tự bảo vệ:** - Phần mềm diệt virus phải có khả năng tự bảo vệ trước các mối nguy cơ từ mã độc, như việc mã độc muốn xóa chương trình diệt virus ra khỏi máy tính. Việc bảo vệ được thực hiện trên file của trương trình trên ổ đĩa, trên RAM và trong Registry. - Ngăn chặn tất cả quá trình điều khiển chương trình diệt virus qua máy tính điều khiển từ xa. - Thiết lập mật khẩu để bảo vệ chương trình khi muốn truy cập hay thực hiện các tác vụ cụ thể. **Chức năng báo cáo** Hỗ trợ báo cáo các thông tin ngay tại máy trạm: Virus quét được; vị trí file nhiễm virus; vị trí file backup; file được backup; trạng thái Start-stop của service theo từng ngày. Hỗ trợ thống kê, báo cáo tình hình virus trên toàn mạng. Hỗ trợ thống kê, báo cáo theo lịch. Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn mạng. Hỗ trợ xuất báo cáo qua nhiều dạng khác nhau" PDF, XLS,… - Các báo cáo phải được phân loại theo mức độ quan trọng. - Các thông báo hệ thống được thực hiện dưới dạng Pop-up trên thanh Taskbar. - Hiển thị nhiều thông tin trên Dashboard. - Các cảnh báo có thể thực hiện qua: Email **Khả năng quản lý tập trung của phần mềm Antivirus** Phần mềm quản trị tập trung hỗ trợ cài đặt trên các hệ điều hành: Microsoft Windows 8,10,11 Server 2008 SP1, Server 2012, Server 2016, Server 2019, Server 2022 Phần mềm quản trị tập trung cho phép triển khai phân cấp theo cơ chế Master/ Slave để phù hợp với các tổ chức lớn. Giao diện phần mềm quản trị có thể cài đặt trên Window,Linux. Hỗ trợ giao diện theo giao diện Web. Hỗ trợ gỡ bỏ các phần mềm từ xa trên các máy Client. Quản lý phần cứng dựa trên các thông tin trên Registry. Có tính năng quản lý moblie android,IOS. Cho phép phản ứng tự động khi phát hiện virus vượt quá giới hạn . Giải pháp chỉ cần một Agent chạy duy nhất quản lý cho các module của chương trình. Giải pháp phải có khả năng tập trung quản lý, triển khai, báo cáo. Khả năng phân chia nhóm quản lý và thiết lập các chính sách quản lý khác nhau. Giải pháp có khả năng cho phép người quản trị kiểm soát ngăn ngừa việc sử dụng License phần mềm Antivirus một cách trái

		phép. Khả năng thiết lập cấu hình Anti-virus, Firewall tới từng máy trạm từ xa và không cho phép người sử dụng bình thường thay đổi các thiết lập này. Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn hệ thống. Chức năng quản lý, áp dụng chính sách không phụ thuộc vào Active Directory. **Khả năng cung cấp tính năng phân tích điều tra nguồn gốc tấn công** Cung cấp khả năng hiển thị rõ ràng hơn về các đối tượng độc hại bằng "thẻ sự cố", mô tả chi tiết quá trình lây nhiễm, với đường lây lan của đối tượng, liệt kê các dữ liệu được thu thập trong thẻ sự cố như: registry, file drop, network Xem toàn bộ phạm vi của bất kỳ mối đe dọa nào. Hiểu nguyên nhân gốc rễ của mối đe dọa và cách nó thực sự xảy ra. Tìm ra đợt tấn công bắt đầu từ đâu? khi nào? mối đe dọa này có còn đang ẩn nấp ở đâu? để loại bỏ các gốc rễ của cuộc tấn công đó. **Yêu cầu bàn giao và cài đặt phần mềm** - Nhà thầu bàn giao sản phẩm và cài đặt, thiết lập cấu hình và quét virus 1 lần sau cài đặt cho máy tính, máy chủ tại Bệnh viện. - Hướng dẫn quản lý, vận hành sử dụng và chuyển giao công nghệ, biên soạn tài liệu hướng dẫn phục vụ vận hành sau này. ***Lưu ý : Thời gian bản quyền là 12 tháng kể từ ngày kích hoạt sản phẩm.*** ***Yêu cầu: dịch vụ triển khai, cài đặt, cấu hình ban đầu cho máy chủ và máy trạm của người dùng, dịch vụ hỗ trợ kỹ thuật trong 12 tháng***

Lưu ý:

- Chào giá phải có ký tên đóng dấu xác thực của Quý Công ty. Đơn vị gửi bảng chào giá đề xuất và giấy đăng ký kinh doanh, hồ sơ năng lực hoạt động thuộc lĩnh vực bắt buộc phải có chứng chỉ hoạt động theo quy định.

- Trong tài liệu của quý công ty khi chào giá vui lòng sử dụng đúng biểu mẫu - KHÔNG xóa, KHÔNG thay đổi thứ tự các cột, các nội dung trong các biểu mẫu đính kèm (biểu mẫu 1). Nội dung nào không có thì quý công ty để trống hoặc ghi không có.

Trân trọng./.

Nơi nhận:
- Như trên;
- Lưu: VT, HCQT (NTT-3b).

GIÁM ĐỐC

SỞ Y TẾ THÀNH PHỐ HỒ CHÍ MINH
BỆNH VIỆN MẮT

Lê Anh Tuấn

Biểu mẫu 1

(Tên Công ty)

BẢNG CHÀO GIÁ

Áp dụng đối với nhu cầu (dịch vụ)/gói thầu ...

Kính gửi: BỆNH VIỆN MẮT

Trên cơ sở yêu cầu **mời chào giá** của BỆNH VIỆN MẮT, chúng tôi .... *[ghi tên, địa chỉ của Công ty]* xin cung cấp chào giá cho **gói thầu/nhu cầu (dịch vụ): ... ,** như sau:

1. Danh mục:

Đơn vị: đồng.

STT	Danh mục thực hiện	ĐVT	Số lượng	Đơn giá (bao gồm thuế, phí)	Thành tiền
	[Lấy thông tin tại khoản 1 và 4 Mục II]				
Tổng cộng					

2. Chào giá này có hiệu lực trong vòng: ... ngày, kể từ ngày phát hành chào giá
3. Thời gian thực hiện: ..... ngày.
4. Chế độ bảo hành: ..... (đối với hàng hóa).
5. Điều kiện thanh toán:
6. Chúng tôi cam kết:

- Không đang trong quá trình thực hiện thủ tục giải thể hoặc bị thu hồi Giấy chứng nhận đăng ký doanh nghiệp hoặc Giấy chứng nhận đăng ký hộ kinh doanh hoặc các tài liệu tương đương khác; không thuộc trường hợp mất khả năng thanh toán theo quy định của pháp luật về doanh nghiệp.
- Những thông tin nêu trong tài liệu trên là trung thực và không vi phạm quy định của pháp luật về cạnh tranh.

....., ngày ..... tháng ..... năm .....

Đại diện hợp pháp của hãng sản xuất, nhà cung cấp

(Ký tên, đóng dấu (nếu có))