

Số: 7115/YCBG-BVT
V/v yêu cầu báo giá gói thầu Mua
sấm, lắp đặt phần mềm diệt virus bản
quyền trong 03 năm

Bắc Ninh, ngày 03 tháng 12 năm 2024

YÊU CẦU BÁO GIÁ

Gói thầu Mua sấm, lắp đặt phần mềm diệt virus bản quyền trong 03 năm
Thuộc dự toán mua sấm: Mua sấm, lắp đặt phần mềm diệt virus bản quyền
trong 03 năm

Kính gửi: Các hãng sản xuất, nhà cung cấp tại Việt Nam

Bệnh viện đa khoa tỉnh Bắc Ninh có nhu cầu tiếp nhận báo giá để tham khảo, xây dựng giá gói thầu, làm cơ sở tổ chức lựa chọn nhà thầu cho gói thầu Mua sấm, lắp đặt phần mềm diệt virus bản quyền trong 03 năm thuộc dự toán mua sấm: Mua sấm, lắp đặt phần mềm diệt virus bản quyền trong 03 năm với nội dung cụ thể như sau:

I. Thông tin của đơn vị yêu cầu báo giá

1. Đơn vị yêu cầu báo giá: Bệnh viện đa khoa tỉnh Bắc Ninh.

Địa chỉ: Đường Nguyễn Quyền - Phường Võ Cường - Thành phố Bắc Ninh
- Tỉnh Bắc Ninh.

2. Thông tin liên hệ của người chịu trách nhiệm tiếp nhận báo giá:

- Họ và tên: Nguyễn Thị Nga

- Chức vụ: Văn thư

- Số điện thoại: 02223821242

- Địa chỉ email: bvdkbacninh@gmail.com

3. Cách thức tiếp nhận báo giá:

Bệnh viện đa khoa tỉnh Bắc Ninh tiếp nhận báo giá theo một trong các cách thức sau:

- Nhận trực tiếp tại địa chỉ: Bệnh viện đa khoa tỉnh Bắc Ninh - Đường Nguyễn Quyền - Phường Võ Cường - Thành phố Bắc Ninh - Tỉnh Bắc Ninh.

- Hoặc nhận qua email (Bản PDF có chữ ký, đóng dấu đỏ Công ty và file excel) theo địa chỉ: bvdkbacninh@gmail.com

4. Thời hạn tiếp nhận báo giá: Từ ngày 03 tháng 12 năm 2024 đến trước 16h30' ngày 16 tháng 12 năm 2024.

Các báo giá nhận được sau thời điểm nêu trên sẽ không được xem xét.

5. Thời hạn có hiệu lực của báo giá: Tối thiểu 90 ngày, kể từ ngày 16 tháng 12 năm 2024.

II. Nội dung yêu cầu báo giá:

1. Danh mục hàng hóa, dịch vụ chi tiết: Theo phụ lục đính kèm
2. Địa điểm cung cấp, lắp đặt; các yêu cầu về vận chuyển, cung cấp, lắp đặt, bảo quản hàng hóa:

- Địa điểm giao hàng: Tại Kho hành chính quản trị và lắp đặt tại các vị trí yêu cầu tại Bệnh viện đa khoa tỉnh Bắc Ninh, Đường Nguyễn Quyền, Phường Võ Cường, Thành phố Bắc Ninh, tỉnh Bắc Ninh.

- Thời gian giao hàng dự kiến: Giao hàng trong vòng 72 giờ kể từ ngày nhận được yêu cầu từ Bệnh viện đa khoa tỉnh Bắc Ninh (Giao hàng trong giờ hành chính, đáp ứng giao hàng, cài đặt kích hoạt phần mềm theo yêu cầu của chủ đầu tư một lần hoặc nhiều lần tùy thuộc thiết bị phần cứng của chủ đầu tư và đưa vào sử dụng nhưng không quá 60 ngày kể từ ngày hợp đồng có hiệu lực đảm bảo hệ thống hoạt động ổn định sau cài đặt).

3. Thời gian thực hiện hợp đồng dự kiến: 36 tháng kể từ ngày hợp đồng có hiệu lực.

4. Dự kiến về các điều khoản tạm ứng, thanh toán hợp đồng:

- Không tạm ứng.
- Thanh toán bằng chuyển khoản.
- Thanh toán trong vòng 90 ngày kể từ ngày hoàn tất các thủ tục thanh toán (hóa đơn, biên bản bàn giao và các chứng từ liên quan) bên mua sẽ chuyển khoản toàn bộ số tiền đã mua hàng hóa cho bên bán.

5. Các thông tin khác (nếu có).

- Chất lượng hàng hoá mới 100%
- Báo giá đã bao gồm các loại thuế, phí, lệ phí (nếu có)... và các khoản chi phí khác có liên quan, bên mua không phải trả thêm bất kỳ khoản chi phí nào khác.

Nơi nhận:

- Như kính gửi;
- Công thông tin điện tử UBND tỉnh (đăng tải);
- Công thông tin điện tử Sở Y tế (đăng tải);
- Phòng CNTT (đăng tải trên website của BV);
- Lưu VT, HĐXD Giá.

GIÁM ĐỐC

Hạ Bá Chân

PHỤ LỤC DANH MỤC HÀNG HÓA

Gói thầu: Mua sắm, lắp đặt phần mềm diệt virus bản quyền trong 03 năm

(Kèm theo Yêu cầu báo giá số 7115/YCBG-BVT ngày 03/12/2024 của Giám đốc Bệnh viện đa khoa tỉnh Bắc Ninh)

Phụ lục 01: Danh mục hàng hóa

STT	Danh mục hàng hóa	Yêu cầu kỹ thuật	Đơn vị tính	Số lượng
1	Mua bản quyền phần mềm diệt virus	- Sử dụng cho 580 máy tính (bao gồm cả máy chủ và máy trạm) - Quản lý bằng phần mềm quản lý tập trung cài trên máy chủ - Yêu cầu kỹ thuật chi tiết tại phụ chi tiết tại phụ lục 02	Bộ bản quyền	01

Phụ lục 02: Yêu cầu kỹ thuật

TT	Nội dung
I	Phần mềm diệt virus cho máy Chủ, máy Trạm
1	Hỗ trợ bảo vệ các hệ điều hành:
1.1	Hệ điều hành Microsoft 7sp1, 8, 10,11
1.2	Hệ điều hành Microsoft Windows Server 2008 sp1, 2012, 2016, 2019,2022
1.3	Có bộ cài bảo vệ cho các hệ điều hành Mobile: iOS, Android
1.4	Hỗ trợ hệ điều hành Linux: Red Hat, CentOS, SuSe, Ubuntu, Debian, AlmaLinux OS, AlterOS, Amazon, Astra,EMIAS, EulerOS, LinuxMint, Oracle,Goslinux...
1.5	Hỗ trợ hệ điều hành MAC từ phiên bản MAC OS X 10.14 hoặc phiên bản mới hơn
2	Chức năng Anti-Virus
2.1	Có khả năng phát hiện và diệt viruses, spyware, worm, trojan rootkit, Keyloger Macro,...
2.2	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.
2.3	Giải pháp hỗ trợ quét thời gian thực các file truy xuất.
2.4	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.
2.5	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.
2.6	Giải pháp có chức năng bảo vệ Web , đáp ứng quét cho traffic web, email, file theo cơ chế chủ động.

2.7	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, SMS và gửi tới SIEM cho người quản trị.
2.8	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.
2.9	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.
2.10	Giải pháp có chức năng Quarantine đối tượng bị nghi lây nhiễm trước khi thực hiện Repair/Delete, khi cần có thể Restore lại từ các file này.
2.11	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
3	Chức năng HIPS (Host IPS)
3.1	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 cập vào tài nguyên hệ điều hành và dữ liệu cá nhân
4	Chức năng giám sát mạng và giám sát hệ thống
4.1	Cho phép xem toàn bộ các kết nối mạng trên máy tính theo thời gian thực.
4.2	Cho phép ghi lại hoạt động của các ứng dụng trên máy tính, cung cấp thông tin này để nâng cao tính bảo mật.
5	Chức năng Firewall
5.1	Phải có chức năng hỗ trợ kiểm soát traffic vào/ra.
5.2	Cho phép thao tác kiểm soát Firewall Client từ xa như: Disable, Enable từ xa.
5.3	Giải pháp phải có khả năng cảnh báo, giám sát các ứng dụng đang chạy.
5.4	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, ICMPv6, IGMP, và GRE.
6	Chức năng Device control
6.1	Phải có khả năng ngăn chặn thiết bị nào có thể hoặc không thể sử dụng trên Windows.
6.2	Phải có khả năng ngăn cấm các ứng dụng chạy từ thiết bị lưu trữ ngoài.
6.3	Phải có khả năng thiết lập lịch được sử dụng thiết bị cấm ngoài qua giao tiếp USB.
6.4	Cho phép thiết lập danh sách các thiết bị cấm ngoài được sử dụng (Trusted Device).
7	Chức năng Web Control
7.1	Lọc Web theo URL, Category, Data, Content.

7.2	Giới hạn truy cập Web theo lịch
7.3	<ul style="list-style-type: none"> - 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.
8	Chức năng Application Control
8.1	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.
8.2	Cho phép tạo ra danh sách trắng các ứng dụng theo nhóm người sử dụng bằng việc kết hợp với AD/LDAP.
8.3	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.
9	Chức năng Virus Update
9.1	Hỗ trợ update bằng tay tại Client từ Server quản lý.
9.2	Hỗ trợ Update cho nhiều Client từ Server quản lý.
9.3	Hỗ trợ lập lịch tự động download update.
9.4	Server quản lý trung gian: Có thể tải Update 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.
9.5	Giao thức dùng để update 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.
10	Chức năng quét lỗ hổng bảo mật
10.1	Có khả năng quét lỗ hổng bảo mật các sản phẩm của Microsoft và các hãng khác.
10.2	Bảo vệ thiết bị khỏi ransomware bao gồm cả các thư mục chia sẻ trên máy chủ (ransomware including protection for server share folders)
10.3	Phục hồi dữ liệu bị nhiễm mã độc (Malicious action rollback)
11	Một số chức năng bảo vệ khác
11.1	Thành phần bảo vệ AMSI hỗ trợ quét phần mềm độc hại từ Microsoft
11.2	<p>Khả năng tự bảo vệ:</p> <ul style="list-style-type: none"> - 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 chương 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 Password để bảo vệ chương trình khi muốn truy cập hay thực hiện các tác vụ cụ thể.
11.3	Tính năng Phát hiện và ngăn chặn các thiết bị USB mô phỏng giả mạo thiết bị bàn phím (BadUSB Attack Prevention)
12	Chức năng Report
12.1	Hỗ trợ report 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.
12.2	Hỗ trợ thống kê, báo cáo tình hình virus trên toàn mạng.
12.3	Hỗ trợ thống kê, báo cáo theo lịch
12.4	Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn mạng
12.5	Hỗ trợ xuất báo cáo qua nhiều dạng khác nhau" PDF, XLS,...
12.6	- 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. - Hiện thị nhiều thông tin trên Dashboard. - Các cảnh báo có thể thực hiện qua: Email
13	Quản lý tập trung
13.1	Phần mềm quản trị tập trung hỗ trợ cài đặt trên các hệ điều hành: Microsoft Windows 7 SP1, 8,10,11 Server 2008 SP1, Server 2012, Server 2016, Server 2019, Server 2022
13.2	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.
13.3	Giao diện phần mềm quản trị có thể cài đặt trên Window,Linux .Hỗ trợ giao diện theo chuẩn MMC của Microsoft và giao diện Web.
13.4	Hỗ trợ gỡ bỏ các phần mềm từ xa trên các máy Client.
13.5	Quản lý phần cứng dựa trên các thông tin trên Registry.
13.6	Có tính năng quản lý mobile android,IOS
13.7	Cho phép phản ứng tự động khi phát hiện virus vượt quá giới hạn
13.8	Giải pháp chỉ cần một Agent chạy duy nhất quản lý cho các module của chương trình.
13.9	Giải pháp phải có khả năng tập trung quản lý, triển khai, báo cáo.
13.10	Khả năng phân chia nhóm quản lý và thiết lập các chính sách quản lý khác nhau.
13.11	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.

13.12	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.
13.13	Hỗ trợ báo cáo, thống kê tình hình cài đặt, trạng thái update virus trên toàn hệ thống.
13.14	Chức năng quản lý, áp dụng chính sách không phụ thuộc vào Active Directory.
13.15	Chức năng xóa dữ liệu từ bộ quản lý tập trung không thể khôi phục được dữ liệu đã xóa.
13.16	Cho phép người dùng có thể điều khiển được phần mềm diệt virus khi ra khỏi mạng của bệnh viện
13.17	Đáp ứng chỉ thị 14/CT-TTg của Thủ tướng chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam
II	Hỗ trợ kỹ thuật
1	Đơn vị cung cấp phần mềm phải có tổng đài hỗ trợ kỹ thuật từ xa tại Việt Nam với thời gian hỗ trợ tất cả các ngày trong tuần (từ 8h sáng đến 10h đêm)
2	Nhân viên trực tổng đài hỗ trợ kỹ thuật phải được đào tạo và có được chứng chỉ từ hãng

(Mẫu Bảng báo giá kèm theo Yêu cầu báo giá ngày 03/12/2024)

CÔNG TY.....

Địa chỉ:.....

Email:.....

Số ĐT liên lạc:.....

BẢNG BÁO GIÁ

Kính gửi: BỆNH VIỆN ĐA KHOA TỈNH BẮC NINH

Địa chỉ: Đường Nguyễn Quyền – Phường Võ Cường – TP Bắc Ninh – Tỉnh Bắc Ninh

Điện thoại: 0222.3.821.242

Email: bvdkbacninh@gmail.com.

1. Công ty/cửa hàng chúng tôi kính gửi quý Bệnh viện báo giá sau:

Stt	STT theo yêu cầu báo giá	Danh mục hàng hoá	Đặc tính kỹ thuật	Đơn vị tính	Số lượng	Ký mã hiệu	Hãng/ Nước sản xuất	Đơn giá	Thành tiền
1									
2									
...									
		Tổng cộng							

(Thành tiền bằng chữ:/.)

(Yêu cầu nhà thầu đính kèm phụ lục đặc tính kỹ thuật của hàng hoá)

- Báo giá đã bao gồm các loại thuế, phí, lệ phí (nếu có)..., và các khoản chi phí khác có liên quan, bên mua không phải trả bất kỳ một chi phí nào khác.
- Hàng hoá mới 100%. Bảo hành theo tiêu chuẩn của nhà sản xuất.....Tháng (nếu có).
- Báo giá này có hiệu lực trong vòng: 90 ngày, kể từ ngày 16/12/2024.
- Chúng tôi cam kết:

- Chịu trách nhiệm về việc cung cấp thông tin về giá của hàng hóa, dịch vụ phù hợp với khả năng cung cấp của mình và bảo đảm việc cung cấp báo giá không vi phạm quy định của pháp luật về cạnh tranh, bán phá giá hoặc nâng khống giá.

- 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.

....., ngày tháng năm 2024

ĐẠI DIỆN ĐƠN VỊ BÁO GIÁ