SỞ Y TẾ ĐỒNG NAI
BỆNH VIỆN ĐA KHOA ĐỒNG NAI

Số: 498 /TM-BVĐKĐN

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

Đồng Nai, ngày 26 tháng 4 năm 2025

THƯ MỜI
V/v chào bảng giá phần mềm diệt virus cho Bệnh viện Đa khoa Đồng Nai.

Kính gửi: Quý nhà thầu quan tâm.

Bệnh viện Đa khoa Đồng Nai có kế hoạch tìm kiếm đơn vị có năng lực phù hợp nhằm thực hiện gói phần mềm diệt virus cho Bệnh viện. Để có cơ sở lập danh mục và xây dựng kế hoạch lựa chọn nhà thầu, Bệnh viện kính mời các nhà thầu quan tâm chào giá các dịch vụ theo danh mục như sau:

(chi tiết theo phụ lục kèm theo)

Yêu cầu chung đối với các nhà thầu:

- Đảm bảo tuân thủ các quy định của Pháp luật hiện hành.
- Có hồ sơ năng lực đầy đủ theo quy định.

Thời hạn nộp báo giá: Từ ngày ra Thư mời đến 16 giờ 30 phút ngày 12 tháng 05 năm 2025

Địa chỉ nhận báo giá: Phòng Công nghệ thông tin (P. 324, lầu 3), bệnh viện Đa khoa Đồng Nai.

Địa chỉ: Số 02 đường Đồng Khởi, phường Bình Đa, thành phố Biên Hòa, tỉnh Đồng Nai

Người liên hệ: Lê Thị Xoang SĐT: 0986712730.

Rất mong được sự quan tâm của các nhà thầu.

Trân trọng.

Nơi nhận:
- Như trên;
- Lưu: VT, CNTT.

GIÁM ĐỐC

SỞ Y TẾ TỈNH ĐỒNG NAI
BỆNH VIỆN ĐA KHOA ĐỒNG NAI

Ngô Đức Tuấn

PHỤ LỤC

(kèm theo Thư mời số: 498/TM-BVĐKĐN ngày 26 tháng 4 năm 2025)

1. Nội dung công việc:

STT		Mô tả
1	**Tính năng quản lý tập trung**	Phần mềm quản trị được cài đặt trên máy chủ quản trị tại doanh nghiệp (on premise);
		Hỗ trợ cài đặt phần mềm quản trị (Security Center) trên các nền tảng hệ điều hành: - Windows: Windows Server 2016, 2019, 2022,… - Hệ điều hành Linux;
		Phân quyền quản trị endpoint theo đơn vị; Endpoint tại đơn vị sẽ giao tiếp với máy chủ đặt tại đơn vị để nhận chính sách, cập nhật bản vá, ...
		Hỗ trợ quản lý, cài đặt từ xa phần mềm của hãng khác trên công cụ quản trị;
		Quản lý, cài đặt, cập nhật các lỗ hổng bảo mật và các bản vá lỗi tập trung hệ điều hành và các phần mềm của thiết bị đầu cuối
		Hỗ trợ quản lý, truy cập các thiết bị đầu cuối, cài đặt từ xa phần mềm của hãng khác trên thiết bị đầu cuối thông qua công cụ quản trị
		Hỗ trợ xác thực 2 yếu tố (Two-factor Authentication) để tăng cường bảo mật
		Quản lý thông tin trên máy chủ/máy trạm/thiết bị thông minh bao gồm các thông tin sau: - Địa chỉ IP, MAC, Tên máy, Hệ điều hành, Thời gian cập nhật gần nhất của Hệ điều hành trên máy chủ/máy trạm; - Trạng thái kết nối đến máy chủ quản trị; - Thông tin bản vá trên máy chủ/máy trạm; - Trạng thái cập nhật thông tin từ máy chủ quản trị; - Chính sách được thiết lập và các vi phạm trên agent.
		Có khả năng điều khiển agent tối thiểu bao gồm các chức năng sau: - Cho phép phân tích, xóa, sửa tệp tin lây nhiễm mã độc trên máy chủ/máy trạm/thiết bị thông minh; - Cho phép điều khiển thay đổi các chính sách phát hiện, ngăn chặn mã độc trên các agent;
		Tính năng báo cáo, thống kê: - Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo; - Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML,…;
2	**Tính năng bảo vệ cho Server:**	
	Phần mềm có khả năng bảo vệ cho các hệ điều hành	Hỗ trợ bảo vệ máy chủ trên các nền tảng hệ điều hành: Windows Server 2012, 2016, 2019, 2022,... và Linux
	Tính năng phòng chống mã độc	Công nghệ Real-time protection, bảo vệ máy chủ theo thời gian thực
		Không cho phần mềm độc hại vô hiệu hóa antivirus; đặt mật khẩu để bảo vệ chương trình; không cho phép bất kỳ thiết bị nào khác điều khiển phần mềm antivirus từ xa ngoại trừ các máy chủ quản trị;

		Quét các tệp tin khi người dùng truy cập ứng dụng, khi tải xuống từ internet hoặc trong quá trình sửa đổi tệp. Công nghệ quét tối ưu, chỉ quét các file mới và các file đã thay đổi so với lần quét trước Cập nhật các dấu hiệu nhận diện mã độc (Domain, IP, hash,…) trên hệ thống quản trị
		Có khả năng phục hồi (restore) trạng thái ban đầu của các tập tin bị phần mềm độc hại can thiệp mã hóa
	Tính năng phát hiện và phản hồi thiết bị đầu cuối (EDR)	Phát hiện sớm các nguy cơ : - Phát hiện tấn công của mã độc dựa theo thông tin: Domain, IP, hash,…; - Giám sát thời gian thực toàn bộ giao tiếp vào và ra máy tính thông qua các Port, địa chỉ IP, ứng dụng,..; Phân tích các hành vi, hoạt động của mã độc trong hệ điều hành để điều tra, xác định nguồn gốc của sự lây nhiễm;
		- Phản hồi với thiết bị đầu cuối khi phát hiện mã độc tấn công: - Đưa ra các phản ứng nhanh với các mối đe dọa phức tạp, tinh vi, đang ẩn nấp trước khi chúng gây ra các thiệt hại; - Cô lập các thiết bị đầu cuối bị nhiễm mã độc ra khỏi mạng; - Tự động cách ly các tập tin độc hại đang ẩn nấp, lây lan khắp hệ thống mạng;.
	Kiểm soát ứng dụng (Application Control)	Quản lý ứng dụng được khởi chạy, ngăn chặn các ứng dụng không mong muốn
		Kiểm soát quyền của ứng dụng được phép truy cập vào hệ thống, giám sát và phân loại ứng dụng.
	Kiểm soát thiết bị ngoại vi (Device Control)	Kiểm soát theo công nghệ truyền dữ liệu (ổ cứng, thiết bị lưu trữ gắn ngoài, máy in, ổ đĩa CD/DVD, …)
		Có chế độ chặn thiết bị kết nối vào máy tính theo lịch hoặc tùy chọn
		Tự động dò quét thiết bị lưu trữ ngoại vi để tìm kiếm mã độc ngay khi được cắm vào máy tính.
	Kiểm soát truy cập web (Web Control)	Thiết lập chính sách hạn chế truy cập web, ngăn chặn việc truy cập các trang web không mong muốn, website độc hại hoặc lừa đảo, kiểm soát việc truy cập theo danh mục website, theo loại dữ liệu hoặc địa chỉ web chỉ định.
	Cập nhật bản vá	Quản lý, cài đặt lỗ hổng bảo mật và bản vá lỗi tập trung của các phần mềm và hệ điều hành Tự động discovery, inventory, notification và tracking tất cả các phần mềm và phần cứng.
	Mã mã hóa dữ liệu	Mã hóa mức File, Folder, Full Disk, ổ đĩa di động (hỗ trợ chế độ Portable File Manager để có thể mở dữ liệu trong ổ đĩa di động bị mã hóa ở các máy tính chưa cài đặt Endpoint).
		Source cài đặt tích hợp vào phân mềm antivirus, không cần một phần mềm mã hóa riêng biệt và được quản lý qua công cụ quản trị tập trung duy nhất.
3	**Tính năng bảo vệ cho máy trạm:**	
	Phần mềm có khả năng bảo vệ cho các hệ điều hành	Hỗ trợ bảo vệ máy chủ trên các nền tảng hệ điều hành: Windows 7 SP1, 8, 10, 11, mobile
	Tính năng phòng chống mã độc	Công nghệ Real-time protection, bảo vệ máy chủ theo thời gian thực
		Không cho phần mềm độc hại vô hiệu hóa antivirus; đặt mật khẩu để bảo vệ chương trình; không cho phép bất

		kỳ thiết bị nào khác điều khiển phần mềm antivirus từ xa ngoại trừ các máy chủ quản trị;
		Quét các tệp tin khi người dùng truy cập ứng dụng, khi tải xuống từ internet hoặc trong quá trình sửa đổi tệp. Công nghệ quét tối ưu, chỉ quét các file mới và các file đã thay đổi so với lần quét trước Cập nhật các dấu hiệu nhận diện mã độc (Domain, IP, hash,…) trên hệ thống quản trị
		Có khả năng phục hồi (restore) trạng thái ban đầu của các tập tin bị phần mềm độc hại can thiệp mã hóa
	Kiểm soát ứng dụng (Application Control)	Quản lý ứng dụng được khởi chạy, ngăn chặn các ứng dụng không mong muốn
		Kiểm soát quyền của ứng dụng được phép truy cập vào hệ thống, giám sát và phân loại ứng dụng
	Kiểm soát thiết bị ngoại vi (Device Control)	Kiểm soát theo công nghệ truyền dữ liệu (ổ cứng, thiết bị lưu trữ gắn ngoài, máy in, ổ đĩa CD/DVD, …)
		Có chế độ chặn thiết bị kết nối vào máy tính theo lịch hoặc tùy chọn
		Tự động dò quét thiết bị lưu trữ ngoại vi để tìm kiếm mã độc ngay khi được cắm vào máy tính
	Kiểm soát truy cập web (Web Control)	Thiết lập chính sách hạn chế truy cập web, ngăn chặn việc truy cập các trang web không mong muốn, website độc hại hoặc lừa đảo, kiểm soát việc truy cập theo danh mục website, theo loại dữ liệu hoặc địa chỉ web chỉ định;

2. Yêu cầu chung đối với các nhà thầu:

- Triển khai và hỗ trợ bảo trì
- Triển khai giải pháp, cài đặt, cấu hình tối ưu sản phẩm trên hệ thống máy trạm, máy chủ.
- Bảo trì, hỗ trợ 12 tháng.

3.Nội dung cần báo giá:

STT	Mặt hàng	Đvt	Số lượng	Đơn giá	Thành tiền
1	Bản quyền chương trình diệt virus cho máy chủ Sever – thời hạn 1 năm	License	20		
2	Bản quyền chương trình diệt virus cho máy trạm – thời hạn 1 năm	License	270		
	Tổng cộng (Bao Gồm VAT và các chi phí theo quy định)				