SỞ Y TẾ TP.HCM
BỆNH VIỆN TAI MŨI HỌNG

Số: 430./TB-BVTMH

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

Thành phố Hồ Chí Minh, ngày 08 tháng 4 năm 2025

THÔNG BÁO
V/v mời báo giá dự toán "Gia hạn phần mềm diệt virus Trenmicro".

Bệnh viện Tai Mũi Họng đang có kế hoạch lựa chọn nhà thầu "Gia hạn phần mềm diệt virus Trenmicro" (theo mẫu đính kèm - Phụ lục 1):

Bệnh viện kính mời các Quý Công ty có năng lực quan tâm gửi đến Bệnh viện chúng tôi bảng báo giá theo danh mục để Bệnh viện làm giá dự toán thực hiện gói thầu này theo đúng quy định.

- Thời gian: từ ngày nhận được thông báo đến ngày 14.../4../2025.

- Lưu ý:

+ Nhà thầu có thể báo giá cho từng mục hoặc toàn bộ gói thầu.
+ Bản báo giá cần ký tên đóng dấu xác nhận của Quý Công ty, để vào bao thư dán kín
+ Ngoài bao thư ghi rõ tên Quý Công ty, người liên hệ và ghi thêm "Bảng báo giá Gia hạn phần mềm diệt virus Trenmicro".
+ Gửi qua văn thư (bảo vệ cổng số 4)

Mọi thắc mắc xin liên lạc về Phòng Hành chính Quản trị Bệnh viện Tai Mũi Họng, số 155B Trần Quốc Thảo, Phường 9, Quận 3, TP.HCM (điện thoại: 028. 3931 7381)

Rất mong được sự quan tâm của Quý Công ty.
Trân trọng./.

Nơi nhận:
- P. QLCL (để kiểm duyệt);
- P. CNTT (đăng tải website BV);
- Lưu: VT, HCQT (PTHA/03b).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

SỞ Y TẾ TP. HỒ CHÍ MINH
BỆNH VIỆN TAI MŨI HỌNG

Khưu Minh Thái

PHỤ LỤC 1

NỘI DUNG MỜI BÁO GIÁ

(Kèm theo Thông báo số 210 /TB-BVTMH ngày 08 tháng 4 năm 2025)

1. Yêu cầu kỹ thuật:

STT	NỘI DUNG YÊU CẦU	MỨC ĐỘ ĐÁP ỨNG	THÔNG SỐ KỸ THUẬT
1	**Quản trị**		
1.1	Quản lý tập trung	Đáp ứng hoàn toàn	Giải pháp cung cấp giao diện quản trị Apex Central duy nhất để quản lý tất cả các chức năng, chính sách và cấu hình
1.2	Triên khai trên nhiều nền tảng như: On-premise, Cloud hoặc kết hợp	Đáp ứng hoàn toàn	Quản trị hệ thống trên cả môi trường on-premises, Cloud, và có khi cả hai đồng thời.
1.3	Hỗ trợ máy trạm Windows/MacOS	Đáp ứng hoàn toàn	Hỗ trợ máy trạm Windows/MacOS và máy chủ Windows
1.4	Hỗ trợ 24/7	Đáp ứng hoàn toàn	Hỗ trợ kỹ thuật đáp ứng SLA 24x7 của hãng Trend Micro
2	**Tính năng**		
2.1	Tính năng DLP xác định hành vi vi phạm chính sách nhằm đáp ứng yêu cầu tuân thủ quy định như HIPAA, PCI-DSS….	Đáp ứng hoàn toàn	- Tính năng Ngăn chặn thất thoát dữ liệu (DLP) giúp định nghĩa những dữ liệu quan trọng và xác định hành vi vi phạm chính sách nhằm đáp ứng yêu cầu tuân thủ quy định như HIPAA, PCI-DSS…. - Tính năng DLP là 1 service tích hợp trực tiếp trên Agent Apex One giúp theo dõi và kiểm soát các hành vi của người dùng trên endpoint. - Cung cấp khả năng kiểm soát, ngăn ngừa thất thoát dữ liệu thông qua các kênh truyền: email client, web mail, SMB, HTTP/HTTPs, ứng dụng IM, ứng dụng Peer-to-Peer, cloud storage service..
2.2	Tính năng Anti-Malware cho phép chống lại các mối đe dọa dạng file như Malware, Virus, Trojan…	Đáp ứng hoàn toàn	- Tính năng Anti-Malware cho phép chống lại các mối đe dọa dạng file như Malware, Virus, Trojan… - Các pattern của cơ sở dữ liệu mối đe dọa được lưu trữ trên máy chủ Trend Micro hoặc được lưu trữ cục bộ. Agent sẽ tải

			xuống định kỳ các mẫu và bản cập nhật chống phần mềm độc hại.
2.3	Bảo vệ lỗ hổng (Vulnerability Protection)	Đáp ứng hoàn toàn	Tính năng Vulnerability Protection phát hiện và bảo vệ máy trạm khỏi các lỗ hổng bảo mật
2.4	Tích hợp máy tính ảo (Vitural Desktop Integration) như VMware Horizon, Citrix XenDesktop	Đáp ứng hoàn toàn	Tính năng Virtual Desktop Integration bảo vệ các môi trường máy tính ảo (virtual desktop environments) như VMware Horizon, Citrix XenDesktop, và Microsoft Remote Desktop Services
2.5	Kiểm soát ứng dụng người dùng cuối (Endpoint Application Control)	Đáp ứng hoàn toàn	Tính năng kiểm soát ứng dụng Application Control và thực thi ứng dụng theo nhu cầu
2.6	Mã hoá ổ cứng sử dụng Microsoft BitLocker/Apple FileVault	Đáp ứng hoàn toàn	- Tính năng Encryption Management for Microsoft BitLocker System cho phép quản lý việc mã hoá ổ cứng máy trạm Windows - Tính năng Encryption Management for Microsoft BitLocker System cho phép quản lý việc mã hoá ổ cứng máy trạm MacOS
2.7	Phòng chống virus cho di động. Phát hiện và ngăn chặn các ứng dụng và dữ liệu nguy hiểm.	Đáp ứng hoàn toàn	- Tính năng Mobile Threat Defense bảo vệ các thiết bị di động, quản lý ứng dụng và bảo vệ dữ liệu. - Phát hiện và ngăn chặn các ứng dụng và dữ liệu nguy hiểm. - Ngăn chặn các nội dung web độc hại sử dụng Web Repuation Services

2. **Số lượng:** 230
3. **Thời hạn:** đến 31/12/2027