SỞ Y TẾ THÀNH PHỐ HỒ CHÍ MINH
BỆNH VIỆN NHI ĐỒNG THÀNH PHỐ

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

Số: 1751/TB-BVNĐTP

Thành phố Hồ Chí Minh, ngày 13 tháng 8 năm 2025

THÔNG BÁO MỜI BÁO GIÁ

Bệnh viện Nhi Đồng Thành Phố đang có kế hoạch thực hiện Gói thầu **"Đầu tư hệ thống bảo mật và bảo mật Cơ sở dữ liệu"**, Yêu cầu nội dung công việc tại Phụ lục 01.

Kính đề nghị các Công ty/ đơn vị quan tâm và có khả năng đáp ứng tiến hành khảo sát gửi báo giá theo mẫu tại Phụ lục 02, để Bệnh viện có cơ sở xây dự toán của gói thầu.

Địa điểm tiếp nhận báo giá:

1. Tên đơn vị : Bệnh viện Nhi Đồng Thành Phố
2. Địa chỉ : Số 15 Võ Trần Chí, Tân Nhựt, TP. Hồ Chí Minh
3. Liên hệ : Bộ phận tiếp nhận văn bản đến - Bệnh viện Nhi Đồng Thành Phố.

- Điện thoại : (028) 22536688.
- Email : bv.nhidong@tphcm.gov.vn

4. Thời hạn nhận báo giá: Trong vòng 05 ngày, từ ngày 14/8/2025 đến hết ngày 19/8/2025.

5. Hình thức nhận báo giá: gửi báo giá qua đường bưu điện.

Mong nhận được sự tham gia của Quý công ty/ đơn vị/nhà cung cấp.

Trân trọng./.

Nơi nhận:
- Ban Giám đốc;
- Các đơn vị cung cấp;
- Đăng website BVNĐTP;
- Lưu: VT, CNTT.
(KL)

GIÁM ĐỐC

SỞ Y TẾ THÀNH PHỐ HỒ CHÍ MINH
BỆNH VIỆN NHI ĐỒNG THÀNH PHỐ

Trương Quang Định

PHỤ LỤC 01: YÊU CẦU NỘI DUNG CÔNG VIỆC

(Kèm theo thông báo mời báo giá ngày 13 /8/2025)

A. YÊU CẦU THIẾT BỊ

Stt	Danh mục hàng hóa/dịch vụ	Đvt	Số lượng	Đơn giá (VNĐ)	Thành tiền (VNĐ)
I	**Thiết bị bảo mật + License**				
1	Thiết bị tường lửa ngoài đính kèm bản quyền phần mềm UTP và dịch vụ hỗ trợ 3 năm. (Firewall External).	Gói	02		
2	Thiết bị tường lửa trong. (Firewall Internal).	Gói	02		
3	Bản quyền phần mềm ATP & dịch vụ bảo hành và hỗ trợ kỹ thuật 3 năm (Cho thiết bị tường lửa trong). (3 Year Advanced Threat Protection)	Gói	02		
II	**Bảo mật Cơ sở dữ liệu**				
	Oracle Database Firewall Và dịch vụ bảo hành hỗ trợ kỹ thuật 3 năm. - Quản lý tình trạng bảo mật cơ sở dữ liệu (Database Security Posture Management). - Quản lý vận hành đơn giản (Simplified Operational Management). - Triển khai Audit Vault. - Triển khai Database Firewall. - Đánh giá an toàn bảo mật định kỳ. - Kiểm toán và giám sát (Audit and Monitor). - Ngăn chặn và bảo vệ (Prevent and Protect). - Báo cáo và cảnh báo (Report and Alert).	Gói	01		
	Tổng cộng (đã bao gồm thuế và các chi phí khác (nếu có))				
	(Bằng chữ:…..)./.				

B. YÊU CẦU KỸ THUẬT:

I.	**Thiết bị bảo mật + License**	
1	**Thiết bị tường lửa ngoài đính kèm bản quyền phần mềm UTP và dịch vụ hỗ trợ 3 năm (Firewall External)**	
1.1	**Năng lực thiết bị tối thiểu bắt buộc**	
1	Kiểu dáng kích thước	Rack Mount, ≤ 1 RU

2	Thông lượng Firewall	≥ 68 Gbps
3	Thông lượng IPS	≥ 12 Gbps
4	Thông lượng Threat Prevention	≥ 10 Gbps
5	Số lượng phiên kết nối đồng thời	≥ 7.800.000 phiên
6	Số lượng phiên kết nối mới/giây	≥ 500.000 phiên
7	Thông lượng IPsec VPN	≥ 50 Gbps
8	Thông lượng SSL/TLS Inspection	≥ 9 Gbps
9	Bộ nhớ lưu trữ	≥ 2 ổ cứng 240 GB
10	Cổng kết nối	≥ 4 cổng 25GE SFP28
		≥ 4 cổng 10GE SFP+
		≥ 8 cổng GE SFP
		≥ 16 cổng GE RJ45
11	Số lượng Firewall ảo tích hợp sẵn có trong bản quyền cho phép và khả năng mở rộng	10/50
12	Nguồn điện	Có ít nhất 2 bộ nguồn có tính năng dự phòng
13	Tính sẵn sàng	Hỗ cơ chế HA (Active-Active, Active-Passive, Clustering) và cho phép HA giữa các Tường lửa ảo trong Cluster.
1.2	**Các tính năng hỗ trợ bắt buộc**	
14	Kiến trúc phần cứng	Có kiến trúc phần cứng với chip xử lý song song hoặc đa nhân, đảm bảo hiệu năng cao để phục vụ đồng thời Firewall và SD-WAN
15	Các tính năng SD-WAN	Hỗ trợ tính năng Apps Control Paths: hơn 3000 ứng dụng
		SLA Health Check theo các thông số Latency, Jitter và Packet Loss
		Hỗ trợ Auto Discovery VPN (ADVPN): tự động thiết lập Tunnel kết nối giữa các Spoke trong kiến trúc Hub và Spoke. Hỗ trợ thiết lập kết nối shortcut giữa các Spoke nằm sau lớp NAT.
		Hỗ trợ link load balancing cho các kết nối Internet

		Monitoring, Report tập trung từ hệ thống quản lý trung tâm
16	Các tính năng kiểm soát ứng dụng (Application Control)	Hỗ trợ nhận diện hơn 5000 ứng dụng theo ít nhất 15 chủ đề (category) khác nhau.
		Hỗ trợ tính năng First Packet Identification, Deep Packet Inspection để hỗ trợ nhận dạng ứng dụng.
		Hỗ trợ kiểm soát từng ứng dụng theo hành vi, chủ đề, mức độ phổ biến, công nghệ, rủi ro, nhà cung cấp, giao thức
17	Các tính năng bảo mật IPS	Hỗ trợ tối thiểu 10,000 IPS signature
		Hỗ trợ phát hiện giao thức bất thường, ngưỡng bất thường, tự định nghĩa signature
		Hỗ trợ dùng phương thức phát hiện: protocol decoder-based, anomaly-based protection, heuristic-based analysis hoặc behavioral patterns
		Hỗ trợ các cách hành xử IPS: hành động mặc định (default), giám sát (monitor), ngăn chặn (block), khởi tạo lại (reset) hoặc cách ly (quarantine)
		Hỗ trợ triển khai ở chế độ: Transparent, In-line, Span mode.
		Hỗ trợ khả năng ngăn chặn tấn công zero-day threats
18	Các tính năng Anti-Malware/Anti-Virus	Ngăn chặn IP Botnet Server với Cơ sở dữ liệu IP Reputation
		Lọc virus thông qua các giao thức và dạng file sau:
		- Hỗ trợ HTTP, FTP, IMAP, POP3, SMTP, NNTP, MAPI, CIFS và SSH
		- Phát hiện dữ liệu mã hóa với SSL Inspection
		Hỗ trợ AI và Sandbox để phát hiện các Virus/Malware nâng cao
19	Các tính năng Web và DNS Filtering	Hỗ trợ tối thiểu 3 chế độ kiểm tra lọc web: Proxy, Flow và DNS.
		Cơ chế lọc web tự động với cơ sở dữ liệu phân loại web theo thời gian thực: tối thiểu 250 triệu URL được đánh giá vào 60 chủ đề (category) web với 60 ngôn ngữ
		Có tính năng chặn, lọc DNS request từ botnet C&C domain

20	Tính năng Gỡ bỏ nội dung độc hại (Content Disarm & Reconstruct - CDR)	Thiết bị phải tích hợp tính năng tự động loại bỏ nội dung nguy hiểm (macro, script ẩn...) trong file văn bản, PDF, zip...và tái cấu trúc file an toàn để đảm bảo người dùng tải về không bị nhiễm mã độc – hoạt động độc lập tại gateway, không yêu cầu cài phần mềm trên thiết bị đầu cuối.
21	Tính năng phân tích file đáng ngờ qua Cloud Sandbox	Hỗ trợ gửi tệp tin đến Cloud Sandbox để thực hiện phát hiện mối đe dọa nâng cao, phân tích các tệp tin và URL trong môi trường đám mây, ứng dụng kỹ thuật phân tích hành vi và học máy để nhận diện các mối đe dọa chưa được biết.
		Hỗ trợ cung cấp khả năng bảo vệ dạng Inline đối với các mối đe dọa chưa được biết đến hoặc zero-day - giữ tập tin lại tối đa 50 giây để chờ kết quả phân tích, và dựa trên kết quả đó, tập tin sẽ được chặn hoặc tiếp tục được truyền đi.
22	Tính năng Mobile Malware Prevention	Thiết bị phải tích hợp khả năng phát hiện và chặn các mối đe dọa mã độc đối với thiết bị di động, sử dụng cơ chế phát hiện dựa trên dấu hiệu đã nhận biết (signature-based) và phân tích hành vi nhằm bảo vệ thiết bị và ngăn ngừa rò rỉ dữ liệu.
1.3	**Bản quyền phần mềm & Bảo hành, dịch vụ hỗ trợ kỹ thuật**	
23	Bản quyền phần mềm & Bảo hành, dịch vụ hỗ trợ kỹ thuật	Bản quyền đầy đủ cho các tính năng IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam, Mobile Malware, Content Disarm & Reconstruct, Cloud Sandbox trong 03 năm. Dịch vụ bảo hành phần cứng và hỗ trợ kỹ thuật đáp ứng SLA 24x7 của hãng sản xuất trong 03 năm.
2	**Thiết bị tường lửa trong (Firewall Internal)**	
2.1	**Năng lực thiết bị tối thiểu bắt buộc**	
1	Kiểu dáng kích thước	Rack Mount, ≤ 1RU
2	Thông lượng Firewall	≥ 68 Gbps
3	Thông lượng IPS	≥ 12 Gbps
4	Thông lượng Threat Prevention	≥ 10 Gbps
5	Số lượng phiên kết nối đồng thời	≥ 7.800.000 phiên
6	Số lượng phiên kết nối mới/giây	≥ 500.000 phiên
7	Thông lượng IPsec VPN	≥ 50 Gbps
8	Thông lượng SSL/TLS Inspection	≥ 9 Gbps

9	Bộ nhớ lưu trữ	≥ 2 ổ cứng 240 GB
10	Cổng kết nối	≥ 4 cổng 25GE SFP28
		≥ 4 cổng 10GE SFP+
		≥ 8 cổng GE SFP
		≥ 16 cổng GE RJ45
11	Số lượng Firewall ảo tích hợp sẵn có trong bản quyền cho phép và khả năng mở rộng	10/50
12	Nguồn điện	Có ít nhất 2 bộ nguồn có tính năng dự phòng
13	Tính sẵn sàng	Hỗ cơ chế HA (Active-Active, Active-Passive, Clustering) và cho phép HA giữa các Tường lửa ảo trong Cluster.
2.2	**Các tính năng hỗ trợ bắt buộc**	
14	Kiến trúc phần cứng	Có kiến trúc phần cứng với chip xử lý song song hoặc đa nhân, đảm bảo hiệu năng cao để phục vụ đồng thời Firewall và SD-WAN
15	Các tính năng SD-WAN	Hỗ trợ tính năng Apps Control Paths: hơn 3000 ứng dụng
		SLA Health Check theo các thông số Latency, Jitter và Packet Loss
		Hỗ trợ Auto Discovery VPN (ADVPN): tự động thiết lập Tunnel kết nối giữa các Spoke trong kiến trúc Hub và Spoke. Hỗ trợ thiết lập kết nối shortcut giữa các Spoke nằm sau lớp NAT.
		Hỗ trợ link load balancing cho các kết nối Internet
		Monitoring, Report tập trung từ hệ thống quản lý trung tâm
16	Các tính năng kiểm soát ứng dụng (Application Control)	Hỗ trợ nhận diện hơn 5000 ứng dụng theo ít nhất 15 chủ đề (category) khác nhau.
		Hỗ trợ tính năng First Packet Identification, Deep Packet Inspection để hỗ trợ nhận dạng ứng dụng.
		Hỗ trợ kiểm soát từng ứng dụng theo hành vi, chủ đề, mức độ phổ biến, công nghệ, rủi ro, nhà cung cấp, giao thức

17	Các tính năng bảo mật IPS	Hỗ trợ tối thiểu 10,000 IPS signature
		Hỗ trợ phát hiện giao thức bất thường, ngưỡng bất thường, tự định nghĩa signature
		Hỗ trợ dùng phương thức phát hiện: protocol decoder-based, anomaly-based protection, heuristic-based analysis hoặc behavioral patterns
		Hỗ trợ các cách hành xử IPS: hành động mặc định (default), giám sát (monitor), ngăn chặn (block), khởi tạo lại (reset) hoặc cách ly (quarantine)
		Hỗ trợ triển khai ở chế độ: Transparent, In-line, Span mode.
		Hỗ trợ khả năng ngăn chặn tấn công zero-day threats
18	Các tính năng Anti-Malware/Anti-Virus	Ngăn chặn IP Botnet Server với Cơ sở dữ liệu IP Reputation
		Lọc virus thông qua các giao thức và dạng file sau:
		- Hỗ trợ HTTP, FTP, IMAP, POP3, SMTP, NNTP, MAPI, CIFS và SSH
		- Phát hiện dữ liệu mã hóa với SSL Inspection
		Hỗ trợ AI và Sandbox để phát hiện các Virus/Malware nâng cao
19	Tính năng Gỡ bỏ nội dung độc hại (Content Disarm & Reconstruct - CDR)	Thiết bị phải tích hợp tính năng tự động loại bỏ nội dung nguy hiểm (macro, script ẩn…) trong file văn bản, PDF, zip…và tái cấu trúc file an toàn để đảm bảo người dùng tải về không bị nhiễm mã độc – hoạt động độc lập tại gateway, không yêu cầu cài phần mềm trên thiết bị đầu cuối.
20	Tính năng phân tích file đáng ngờ qua Cloud Sandbox	Hỗ trợ gửi tệp tin đến Cloud Sandbox để thực hiện phát hiện mối đe dọa nâng cao, phân tích các tệp tin và URL trong môi trường đám mây, ứng dụng kỹ thuật phân tích hành vi và học máy để nhận diện các mối đe dọa chưa được biết.
		Hỗ trợ cung cấp khả năng bảo vệ dạng Inline đối với các mối đe dọa chưa được biết đến hoặc zero-day - giữ tập tin lại tối đa 50 giây để chờ kết quả phân tích, và dựa trên kết quả đó, tập tin sẽ được chặn hoặc tiếp tục được truyền đi.
21	Tính năng Mobile Malware Prevention	Thiết bị phải tích hợp khả năng phát hiện và chặn các mối đe dọa mã độc đối với thiết bị di động, sử dụng cơ chế phát hiện dựa trên dấu hiệu đã nhận biết (signature-based) và phân tích hành vi nhằm bảo vệ thiết bị và ngăn ngừa rò rỉ dữ liệu.

3	**Bản quyền phần mềm ATP & dịch vụ bảo hành và hỗ trợ kỹ thuật 3 năm (cho**	
22	Bản quyền phần mềm & Bảo hành, dịch vụ hỗ trợ kỹ thuật	Bản quyền đầy đủ cho các tính năng IPS, Advanced Malware Protection, Application Control, Mobile Malware, Content Disarm & Reconstruct, Cloud Sandbox trong 03 năm. Dịch vụ bảo hành phần cứng và hỗ trợ kỹ thuật đáp ứng SLA 24x7 của hãng sản xuất trong 03 năm.
II.	**Bảo mật Cơ sỡ dữ liệu**	
A	**Các tính năng hỗ trợ bắt buộc**	
1	Quản lý tình trạng bảo mật cơ sở dữ liệu (Database Security Posture Management)	Đánh giá và phát hiện dữ liệu nhạy cảm, đánh giá mức độ bảo vệ và giám sát người truy cập. Cung cấp cái nhìn tổng quan, đơn giản hóa về các đánh giá bảo mật cơ sở dữ liệu và các rủi ro liên quan. Xác định các lỗ hổng và tăng cường khả năng phòng thủ.
2	Kiểm toán và giám sát (Audit and Monitor)	Thu thập và hợp nhất dữ liệu kiểm toán từ nhiều nguồn: Cơ sở dữ liệu (Oracle Database, Microsoft SQL Server, SAP Sybase, IBM DB2 for LUW, MySQL), hệ điều hành (Linux, IBM AIX, Oracle Solaris, Microsoft Windows), dịch vụ thư mục (Microsoft Active Directory), hệ thống tệp tin và dữ liệu kiểm toán tùy chỉnh.
		Giám sát hoạt động cơ sở dữ liệu theo thời gian thực để phản ứng nhanh chóng với các sự kiện bảo mật.
		Phát hiện và ngăn chặn các cuộc tấn công SQL Injection và các hoạt động trái phép.
		Theo dõi sự thay đổi của các thủ tục lưu trữ (stored procedures) và quản lý quyền truy cập của người dùng.
3	Báo cáo và cảnh báo (Report and Alert)	Cung cấp các báo cáo mặc định và tùy chỉnh cho các quy định tuân thủ như GDPR, PCI DSS, HIPAA, SOX.
		Khả năng tạo báo cáo dạng PDF/Excel
		Hỗ trợ phân tích pháp y (forensic analysis) và điều tra sự cố
		Tạo cảnh báo dựa trên quy tắc cho các sự kiện kiểm toán và gửi thông báo
4	Ngăn chặn và bảo vệ (Prevent and Protect)	Tường lửa cơ sở dữ liệu đa tầng kiểm tra lưu lượng SQL để phát hiện và tùy chọn chặn các SQL trái phép.
		Thực thi đường dẫn đáng tin cậy (trusted path enforcement) đến cơ sở dữ liệu dựa trên người dùng OS, chương trình

		client, IP client và danh mục SQL
		Công cụ chính sách mạnh mẽ phát hiện truy cập trái phép vào các bảng nhạy cảm
5	Quản lý vận hành đơn giản (Simplified Operational Management)	Triển khai dưới dạng thiết bị phần mềm (software appliance).
		Quản lý tập trung triển khai AVDF với bảo mật nhúng.
		Kiến trúc có khả năng mở rộng cao với tính sẵn sàng cao (High Availability) và phục hồi thảm họa (Disaster Recovery)
		Hỗ trợ thu thập bản ghi kiểm toán không cần tác nhân (agentless) cho Oracle và Microsoft SQL Server
B	**Dịch vụ triển khai**	
1	**Triển khai Audit Vault**	Cài đặt server Audit Vault
		Tạo các user quản lý Audit Vault
		Cài đặt Audit Vault agent trên các DB server
		Đăng kí máy chủ Database với Audit Vault và kích hoạt
		Kích hoạt tính năng audit trên Database
		Tạo User trên Database cho việc thu thập Audit data
		Cài đặt Audit Vault agent trên các DB server
		Cấu hình thu thập thông tin audit trail trên các Database Target
		Thực hiện định nghĩa và bật Unified Auditing
		Khởi tạo các chính sách unified auditing
		Quản lí dữ liệu Audit từ các Target Database
		Cấu hình các cảnh báo chủ động theo dõi các hoạt động trên hệ thống CSDL
		Cấu hình các report lịch sử các hoạt động hoạt động Database
		Cấu hình theo dõi hoạt động Database Firewall
		Tài liệu cài đặt, hướng dụng sử dụng
2	**Triển khai Database Firewall**	Cài đặt server Database Firewall

		Tạo các user quản lý Database Firewall
		Đăng kí Database Firewall với Audit Vault và cấu hình Proxy
		Cấu hình các Database với Database Firewall
		Cấu hình các chính sách cảnh báo trên Database Firewall về các hoạt động nguy hiểm trên Database
		Cấu hình các report về phân quyền, hoạt động,... trên các Database
		Cấu hình để ngăn chặn các hoạt động bất thường trước khi đến Database
		Cấu hình ngăn chặn những connection, application, IP,... không cho phép và được phép kết nối đến Database
		Cấu hình phân quyền cho nhóm người dùng có thể thực hiện những hoạt động gây tổn hại đến data của Database
		Cấu hình phân quyền cho nhóm người dùng không thể thực hiện những hoạt động gây tổn hại đến data của Database
		Tài liệu cài đặt, hướng dụng sử dụng
3	**Đánh giá an toàn bảo mật định kỳ**	
		Đánh giá an toàn thông tin tài khoản người dùng
		Đánh giá cấp phát quyền và các role trên hệ thống CSDL Oracle
		Đánh giá quản lý truy cập vào hệ thống
		Đánh giá kiểm soát truy cập fine-grained access
		Đánh giá hoạt động theo dõi người dùng
		Đánh giá mức độ mã hóa dữ liệu.
		Đánh giá lạm dụng quyền và khả năng leo thang.
		Đánh giá khả năng bảo vệ tập tin và các data files.
		Đánh giá an toàn bảo mật Oracle Net
		Đánh giá các thông số Oracle Database
		Đánh giá bảo mật Data Dictionary
		Đánh giá cấu hình an toàn bảo mật CSDL

		Đánh giá các thông số bảo mật trên hệ điều hành của CSDL Oracle
		Phân tích báo cáo các vấn đề an toàn bảo mật
		Đánh giá khả năng xâm nhập từ bên ngoài
		Đánh giá khả năng xâm nhập từ bên trong
		Tư vấn các giải pháp an toàn bảo mật phù hợp, giúp ngăn chặn các vấn đề có thể xảy ra.
		Đánh giá các lỗ hổng bảo mật và khuyến cáo các bản vá.
		Báo cáo phân tích và khuyến nghị.
C	**Bảo hành và dịch vụ đi kèm**	
1	Bản quyền phần mềm	03 năm với đầy đủ các tính năng và các bản cập nhật
2	Bảo hành, dịch vụ hỗ trợ kỹ thuật	Dịch vụ bảo hành phần cứng và hỗ trợ kỹ thuật đáp ứng SLA 24x7 trong 03 năm.

PHỤ LỤC 02: MẪU BÁO GIÁ DỊCH VỤ

(Kèm theo thông báo mời báo giá ngày 18 /8/2025)

TÊN ĐƠN VỊ CUNG CẤP

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

....., ngày.....tháng.....năm 2025

BẢNG BÁO GIÁ

Kính gửi: Bệnh viện Nhi Đồng Thành Phố

Tên đơn vị:.....

Địa chỉ:.....

Giấy phép kinh doanh số.....được cấp bởi.....

Căn cứ thông báo mời báo giá của Bệnh viện Nhi Đồng Thành Phố và khả năng cung cấp của công ty....., chúng tôi xin gửi tới quý Bệnh viện báo giá cho "Đầu tư hệ thống bảo mật và bảo mật Cơ sở dữ liệu" như sau:

Đvt: đồng

Stt	Danh mục dịch vụ	Đvt	Số lượng	Đơn giá	Thành tiền	Thời gian thực hiện
(1)	(2)	(3)	(4)	(5)	(6=4*5)	(7)
01						36 tháng
Tổng cộng sau thuế						

Báo giá có hiệu lực từ ngày.....

Đại diện hợp pháp của đơn vị báo giá