BỘ Y TẾ
BỆNH VIỆN PHONG - DA LIỄU TRUNG ƯƠNG QUY HÒA

Số: 1260/TWQH-CNTT
V/v Mời báo giá cung cấp Hệ thống giám sát mạng

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

Gia Lai, ngày 19 tháng 8 năm 2026

YÊU CẦU BÁO GIÁ

Kính gửi: Các đơn vị cung cấp tại Việt Nam.

Bệnh viện Phong - Da liễu Trung ương Quy Hòa có nhu cầu tiếp nhận báo giá để làm cơ sở tham khảo, xây dựng giá gói thầu cho kế hoạch lựa chọn nhà thầu cung cấp hệ thống giám sát mạng với nội dung cụ thể như sau:

1. Đơn vị yêu cầu báo giá

- Bệnh viện Phong - Da liễu Trung ương Quy Hòa; Địa chỉ: Phường Quy Nhơn Nam, Tỉnh Gia Lai.
- Thư mời báo giá cung cấp hệ thống giám sát mạng được đăng tải trên cổng thông tin điện tử website: "www.bvquyhoa.vn" và "muasamcong.mpi.gov.vn".

2. Cách thức tiếp nhận báo giá

- Nhận trực tiếp:
+ Phòng Văn thư, Bệnh viện Phong - Da liễu Trung ương Quy Hòa;
+ Địa chỉ: Phường Quy Nhơn Nam, Tỉnh Gia Lai;
+ Số điện thoại: 0256. 3747999.
- Nhận qua email: quyhoandh2005@gmail.com

3. Thời hạn tiếp nhận báo giá: Từ ngày ra thông báo đến hết ngày 25/8/2026. Các báo giá nhận sau thời điểm nêu trên sẽ không được xem xét.

4. Thời hạn có hiệu lực của báo giá: Tối thiểu 90 ngày.

5. Nội dung yêu cầu báo giá:

STT	Danh mục hàng hóa/dịch vụ	Yêu cầu kỹ thuật và phạm vi dịch vụ	Số lượng	ĐVT
1	Hệ thống giám sát mạng	Chi tiết tại Phụ lục kèm theo	01	Hệ thống

6. Điều khoản thanh toán

- Đồng tiền thanh toán: VND.
- Thanh toán hợp đồng: Thanh toán 100% giá trị hợp đồng trong vòng 30 ngày, sau khi Bệnh viện nhận được đầy đủ các giấy tờ thanh toán: Biên bản nghiệm thu đưa vào sử dụng, hóa đơn tài chính và các giấy tờ liên quan kèm theo.
- Phương thức thanh toán: chuyển khoản.

Xin trân trọng cảm ơn./.

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

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỆNH VIỆN PHONG DA LIỄU TRUNG ƯƠNG QUY HÒA

Nguyễn Đăng Vinh

BỘ Y TẾ
BỆNH VIỆN PHONG - DA LIỄU TRUNG ƯƠNG QUY HÒA

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

PHỤ LỤC YÊU CẦU KỸ THUẬT VÀ PHẠM VI DỊCH VỤ

(Kèm theo Thư mời báo giá số: 1260 */TWQH-CNTT, ngày 19 /8/2026*
của Bệnh viện Phong - Da liễu Trung ương Quy Hòa)

Yêu cầu kỹ thuật và phạm vi dịch vụ:

1. Dịch vụ giám sát và quản lý an toàn thông tin (Managed Security Services - MSS)

Dịch vụ được cung cấp theo mô hình dịch vụ quản lý an toàn thông tin tập trung, bao gồm các thành phần triển khai tại hệ thống của khách hàng và các thành phần xử lý, giám sát tập trung tại Trung tâm điều hành an toàn thông tin (SOC) của nhà cung cấp.

Để tăng cường khả năng thu thập và giám sát các sự kiện trên hạ tầng CNTT của Bệnh viện, dịch vụ MSS thực hiện thu thập, tập trung và phân tích log từ các nguồn thuộc phạm vi giám sát. Cụ thể, bao gồm các thành phần:

Thành phần thu thập và chuyển tiếp sự kiện (Event Collector – EC hoặc thành phần tương đương): Có chức năng thu nhận, tập trung, chuẩn hóa và chuyển tiếp nhật ký (log), sự kiện từ các nguồn trong hệ thống CNTT của Bệnh viện. Việc tích hợp các nguồn log cụ thể được xác định trên cơ sở khảo sát hiện trạng và phạm vi hệ thống CNTT của Bệnh viện; nhà cung cấp có trách nhiệm đề xuất phương án kết nối, thu thập và giám sát phù hợp

Thành phần giám sát và phân tích lưu lượng mạng (Network Sensor hoặc thành phần tương đương): Có chức năng thu thập và phân tích lưu lượng mạng thông qua cơ chế SPAN, Network TAP hoặc phương thức tương đương tại các vị trí phù hợp trên hệ thống mạng; thực hiện phân tích sự kiện và lưu lượng để phát hiện hành vi bất thường, dấu hiệu nguy cơ và các cuộc tấn công vào hệ thống.

Dữ liệu, sự kiện và thông tin phân tích từ các thành phần thu thập/giám sát được truyền về hệ thống xử lý, giám sát tập trung của nhà cung cấp để tương quan, phân tích và quản lý cảnh báo.

Các chức năng giám sát, phát hiện và phân tích bao gồm:

- Phát hiện sớm các hành vi bất thường trong hệ thống mạng;
- Phát hiện các kết nối đến/đi từ máy chủ có dấu hiệu liên quan đến mã độc;
- Phát hiện hoạt động dò quét, thăm dò hệ thống;
- Phát hiện các dấu hiệu tấn công vào hệ thống cơ sở dữ liệu;
- Phát hiện các dấu hiệu, hành vi liên quan đến Phishing;
- Phát hiện các dấu hiệu liên quan đến Shellcode;
- Giám sát, phát hiện các hành vi tấn công nhằm vào thiết bị IoT;
- Hỗ trợ lưu trữ gói tin phục vụ công tác phân tích, điều tra và truy vết sự cố;

- Thống kê, nhận diện các phần mềm độc hại được phát hiện trong hệ thống CNTT;
- Phát hiện các dấu hiệu khai thác lỗ hổng bảo mật, bao gồm các lỗ hổng được định danh theo mã CVE;
- Phát hiện các hành vi vi phạm chính sách an toàn thông tin và các dấu hiệu tấn công;
- Hỗ trợ phân loại, ánh xạ các hành vi tấn công theo MITRE ATT&CK hoặc phương thức phân loại tương đương.

Thành phần xử lý, giám sát tập trung tại Trung tâm điều hành an toàn thông tin (SOC): Bao gồm hệ thống xử lý sự kiện tập trung và các nền tảng/công cụ hỗ trợ giám sát, phân tích, phát hiện và ứng phó sự cố. Các dịch vụ chuyên sâu như Threat Intelligence, Threat Hunting, Incident Response và Digital Forensics được cung cấp theo phạm vi dịch vụ và yêu cầu thực tế.

1.1 Phạm vi triển khai và quy mô giám sát

STT	Yêu cầu kỹ thuật	Mô tả chi tiết
1.1	**Máy chủ (Servers)**	- Tổng số **07 máy chủ Windows/Linux** thuộc phạm vi giám sát.
1.2	**Phạm vi giám sát**	- Thu thập log từ **07 máy chủ Windows/Linux** thông qua agent hoặc thành phần thu thập log phù hợp. - Thu thập log từ các thiết bị/hệ thống hỗ trợ thông qua **Syslog hoặc phương thức kết nối tương đương**, tùy thuộc khả năng tích hợp của từng thiết bị. - Phạm vi và danh sách nguồn log cụ thể được xác định trên cơ sở khảo sát hiện trạng và thống nhất giữa Bệnh viện với nhà cung cấp. - Giám sát tối thiểu 200 EPS (Events Per Second – Sự kiện trên giây).
1.3	**Thời gian cung cấp dịch vụ**	**24 tháng** kể từ ngày nghiệm thu đưa dịch vụ vào vận hành hoặc theo thời gian được quy định trong hợp đồng.

1.2 Yêu cầu về thời gian và phương thức giám sát:

Dịch vụ phải thực hiện giám sát an toàn thông tin liên tục 24 giờ/ngày, 7 ngày/tuần trong thời gian cung cấp dịch vụ.

Có đội ngũ chuyên trách tiếp nhận, phân tích và xử lý/cùng phối hợp xử lý các cảnh báo, sự cố phát sinh.

Có cơ chế thông báo cảnh báo và phối hợp xử lý sự cố với đầu mối của Bệnh viện.

Có khả năng cung cấp báo cáo định kỳ và báo cáo đột xuất theo yêu cầu.

2. Yêu cầu về giám sát, phát hiện, cảnh báo và hỗ trợ xử lý sự cố an toàn thông tin:

STT	Thông tin giám sát	Chi tiết
I	**Giám sát, phát hiện, cảnh báo (Security Monitoring)**	
1.	Đăng nhập, login/logout	- Đăng nhập sai nhiều lần - Đăng nhập thời điểm bất thường (Ngày nghỉ, lễ, ngoài giờ, ban đêm..) - Đăng nhập từ địa chỉ IP, khu vực địa lý hoặc nguồn truy cập bất thường theo chính sách/định tuyến được xác định - Đăng nhập bằng tài khoản không hợp lệ, tài khoản hết hạn, bị khóa hoặc không còn được phép sử dụng - Đăng nhập đồng thời hoặc bất thường từ nhiều địa chỉ IP/nguồn truy cập đối với cùng một tài khoản - Đăng nhập từ nhiều IP vào 01 nguồn - Đăng nhập từ nhiều nguồn vào 01 IP
2.	Dò quét, thăm dò và Brute Force	- Phát hiện hoạt động dò quét, thăm dò hệ thống và dịch vụ mạng; - Phát hiện hoạt động dò quét tài khoản, mật khẩu hoặc thông tin xác thực; - Phát hiện các hành vi thử nhiều mật khẩu/tài khoản trong thời gian ngắn (Brute Force); - Phát hiện việc sử dụng các công cụ, script hoặc payload có dấu hiệu phục vụ hoạt động dò quét, khai thác hoặc tấn công; - Phát hiện các hành vi dò quét mạng, dịch vụ, tài khoản mặc định hoặc thông tin xác thực yếu.
3.	Thay đổi cấu hình, tài khoản và tính toàn vẹn hệ thống	- Phát hiện việc tạo mới, thay đổi, vô hiệu hóa hoặc xóa tài khoản người dùng; - Phát hiện thay đổi mật khẩu và thông tin xác thực; - Phát hiện thay đổi, sửa hoặc xóa tệp tin/cấu hình hệ thống; - Giám sát các sự kiện audit của hệ thống và các thao tác quản trị có dấu hiệu bất thường; - Phát hiện các thay đổi được thực hiện tại thời điểm hoặc từ nguồn truy cập bất thường; - Giám sát tính toàn vẹn của các tệp tin, thư mục hoặc thành phần hệ thống được cấu hình giám sát; - Phát hiện các tiến trình có dấu hiệu bất thường về hành vi hoặc việc sử dụng tài nguyên máy chủ; - Phát hiện các dấu hiệu của Phishing và cài đặt/phát tán mã độc thông qua ứng dụng hoặc hệ thống được giám sát.

STT	Thông tin giám sát	Chi tiết
4.	Kết nối bất thường và dấu hiệu tấn công từ chối dịch vụ	- Phát hiện kết nối tới/đến từ các địa chỉ IP, domain, URL hoặc nguồn được xác định có nguy cơ theo các nguồn Threat Intelligence được tích hợp/khai thác trong dịch vụ; - Phát hiện các kết nối bất thường tới các dịch vụ, cổng quản trị hoặc cổng dữ liệu theo chính sách giám sát; - Phát hiện các kết nối bất thường liên quan đến các giao thức/dịch vụ như SMB, RDP, SSH, Telnet, Database và các dịch vụ mạng khác; - Phát hiện các kết nối đồng thời, tần suất hoặc lưu lượng tăng bất thường; - Phát hiện dấu hiệu kết nối bất thường tới các máy chủ DNS, NTP hoặc các dịch vụ Internet bên ngoài; - Phát hiện các dấu hiệu tấn công DoS/DDoS dựa trên lưu lượng, tần suất kết nối, nguồn phát sinh và các đặc điểm bất thường khác.
5.	Phát hiện các hành vi tấn công ứng dụng Web	- Phát hiện các dấu hiệu tấn công ứng dụng Web như XSS, SQL Injection, CSRF, Path Traversal, RFI/LFI và các hình thức tấn công tương tự; - Phân tích các sự kiện có payload, signature hoặc dấu hiệu hành vi tương ứng với các nhóm tấn công ứng dụng Web; - Hỗ trợ phân loại/đối chiếu các hành vi tấn công theo OWASP khi có đủ thông tin.
6.	Phát hiện và thống kê Malware/ Botnet	- Phát hiện các kết nối tới các máy chủ điều khiển Botnet/C&C; - Phát hiện các địa chỉ IP/domain/URL có dấu hiệu liên quan đến mã độc hoặc nằm trong nguồn thông tin nguy cơ; - Phát hiện các file, URL hoặc nội dung có dấu hiệu độc hại được truyền qua môi trường mạng; - Phát hiện các Shellcode, payload hoặc hành vi có dấu hiệu khai thác lỗ hổng phần mềm/dịch vụ; - Thống kê, phân loại các mối đe dọa Malware/Botnet được phát hiện trong phạm vi hệ thống giám sát.
7.	Phát hiện dấu hiệu khai thác lỗ hổng và cảnh báo nguy cơ	- Phát hiện các dấu hiệu khai thác lỗ hổng bảo mật trên hệ thống, máy chủ và dịch vụ; - Đối chiếu các dấu hiệu tấn công với thông tin lỗ hổng đã được công bố, bao gồm mã định danh CVE khi có đủ thông tin; - Cảnh báo các hệ thống/dịch vụ có dấu hiệu đang bị khai thác hoặc có nguy cơ liên quan đến lỗ hổng bảo mật
8.	Giám sát trạng thái và mức độ tuân thủ	- Giám sát trạng thái của các Endpoint được tích hợp/đăng ký vào hệ thống; - Phát hiện các Endpoint không đáp ứng chính sách bảo mật được cấu hình, như trạng thái Antivirus/EDR, Firewall hoặc

STT	Thông tin giám sát	Chi tiết
	của các Endpoint được tích hợp vào dịch vụ	các yêu cầu bảo mật khác; - Cảnh báo các Endpoint có trạng thái bất thường hoặc không tuân thủ chính sách bảo mật; - Cung cấp thống kê tổng hợp về tình trạng tuân thủ của các Endpoint được giám sát.

3. Yêu cầu về các tính năng hỗ trợ quản lý, giám sát và xử lý sự cố:

3.1. Tính năng điều phối, quản lý và hỗ trợ phản ứng xử lý sự cố an toàn thông tin:

STT	Tên tính năng
1	**Tiếp nhận, tập trung và quản lý các cảnh báo, sự kiện an toàn thông tin** từ hệ thống SIEM và/hoặc các thành phần giám sát, phát hiện thuộc phạm vi dịch vụ.
2	**Phân loại, đánh giá và xác định mức độ ưu tiên/mức độ nghiêm trọng** của cảnh báo, sự cố theo các tiêu chí được cấu hình và thống nhất trong phạm vi dịch vụ.
3	**Tạo lập, lập lịch, tổng hợp và xuất báo cáo** về tình hình cảnh báo, sự cố và hoạt động xử lý thông qua giao diện quản lý.
4	**Quản lý Ticket xử lý sự cố**, hỗ trợ tạo, cập nhật, phân công/gán đơn vị hoặc người xử lý, theo dõi trạng thái và lịch sử xử lý theo cơ cấu tổ chức.
5	**Thiết lập, quản lý và theo dõi SLA** đối với cảnh báo/sự cố theo mức độ nghiêm trọng, phạm vi dịch vụ và yêu cầu xử lý được thống nhất trong hợp đồng.
6	**Gửi thông báo** khi phát sinh Ticket mới, khi có thay đổi trạng thái và khi Ticket sắp đến hoặc vượt thời hạn xử lý theo SLA.
7	**Thống kê, theo dõi các chỉ số KPI** liên quan đến hoạt động tiếp nhận, phân tích và xử lý cảnh báo/sự cố theo đơn vị, nhóm hoặc người xử lý.
8	**Theo dõi thời gian tiếp nhận, phản hồi và xử lý cảnh báo/sự cố**, hỗ trợ đánh giá mức độ đáp ứng SLA và hiệu quả xử lý.

3.2. Các kịch bản phát hiện và phân tích lưu lượng mạng:

STT	Tên tính năng
1	**Phát hiện dấu hiệu tấn công từ chối dịch vụ (DoS/DDoS):** Có khả năng phát hiện các dấu hiệu bất thường về lưu lượng, bao gồm sự gia tăng đột biến lưu lượng hoặc số lượng kết nối/yêu cầu trong khoảng thời gian ngắn; phát hiện các mẫu lưu lượng bất thường liên quan đến các giao thức như TCP/SYN, ICMP, HTTP và các giao thức phù hợp khác.
2	**Phát hiện dấu hiệu rà quét, dò tìm dịch vụ và lỗ hổng:** Có khả năng

STT	Tên tính năng
	phát hiện các hành vi rà quét cổng, dò tìm dịch vụ, xác định hệ thống/phiên bản dịch vụ và các dấu hiệu kiểm tra khả năng khai thác lỗ hổng trên hệ thống mạng.
3	**Phát hiện dấu hiệu tấn công APT và các hành vi xâm nhập có chủ đích:** Có khả năng phát hiện các hành vi bất thường trong lưu lượng mạng, các kết nối đáng ngờ giữa hệ thống nội bộ và bên ngoài, hành vi truy cập bất thường vào các hệ thống quan trọng và kết hợp thông tin tình báo mối đe dọa (Threat Intelligence) để hỗ trợ nhận diện nguy cơ.
4	**Phát hiện dấu hiệu khai thác dịch vụ và lỗ hổng:** Có khả năng phát hiện các dấu hiệu khai thác dịch vụ/lỗ hổng thông qua phân tích lưu lượng, hành vi kết nối, mẫu dữ liệu và các dấu hiệu khai thác đã được nhận diện; hỗ trợ đối chiếu với thông tin lỗ hổng đã biết, bao gồm mã CVE khi có đủ thông tin xác định.
STT	**Tên tính năng**

3.3. Yêu cầu đối với giao diện Dashboard giám sát, thống kê và quản lý sự cố:

STT	Tên tính năng
1	Biểu đồ sự kiện an toàn thông tin thời gian thực: Hiển thị số lượng sự cố mở mới và sự cố đã xử lý theo từng ngày. Điều này giúp theo dõi xu hướng sự cố và đánh giá hiệu quả xử lý theo thời gian.
2	Các card visual biểu diễn số lượng của tất cả các sự cố, các sự cố đang mở, các loại sự cố đã được phân loại.
3	Biểu đồ phân loại mức độ ưu tiên/mức độ nghiêm trọng của sự cố, cho phép phân loại và theo dõi theo các mức độ phù hợp với chính sách phân loại sự cố được thống nhất.
4	Hệ thống Dashboard cung cấp các bảng dữ liệu giúp hiển thị chi tiết thông tin về từng sự cố, hỗ trợ người quản lý theo dõi và xử lý nhanh chóng.
5	Bộ lọc thời gian: Người dùng có thể chọn khoảng thời gian thống kê để hiển thị dữ liệu theo nhu cầu, giúp phân tích hiệu suất xử lý sự cố trong các giai đoạn khác nhau.

3.4. Xác thực đa yếu tố (MFA) đối với tài khoản quản trị và người dùng hệ thống.

4. Các dịch vụ chuyên sâu trong phạm vi MSS

4.1. Dịch vụ ứng cứu xử lý sự cố.

Nhà cung cấp thực hiện dịch vụ hỗ trợ ứng cứu và xử lý sự cố an toàn thông tin trong phạm vi hợp đồng, bao gồm:

- Xác định, phân loại và đánh giá phạm vi, mức độ ảnh hưởng của sự cố;
- Phối hợp thu thập và phân tích thông tin, bằng chứng liên quan;
- Hướng dẫn hoặc trực tiếp phối hợp thực hiện các biện pháp ngăn chặn, giảm thiểu và khắc phục sự cố theo phạm vi dịch vụ;
- Hỗ trợ loại bỏ nguyên nhân/mã độc và khôi phục hoạt động của hệ thống;
- Đánh giá nguy cơ tái diễn;
- Đưa ra báo cáo và khuyến nghị tăng cường an toàn thông tin sau sự cố.

4.2. Dịch vụ điều tra số.

Nhà cung cấp có khả năng thực hiện điều tra, phân tích và bảo toàn bằng chứng số nhằm xác định nguyên nhân, nguồn gốc, phạm vi ảnh hưởng và phương thức thực hiện của sự cố an toàn thông tin.

Phạm vi điều tra có thể bao gồm máy chủ, thiết bị đầu cuối, thiết bị mạng, lưu lượng mạng, cơ sở dữ liệu, thư điện tử, mã độc, bộ nhớ và các nguồn bằng chứng số phù hợp với từng sự cố.

Kết quả điều tra phải bao gồm báo cáo kết quả phân tích và các khuyến nghị xử lý, khắc phục.

4.3. Dịch vụ săn tìm mối nguy (Threat Hunting).

Nhà cung cấp có khả năng thực hiện săn tìm chủ động các mối đe dọa tiềm ẩn trong hạ tầng CNTT của Bệnh viện dựa trên thông tin tình báo mối đe dọa, IoC/IoA, TTP và các dấu hiệu bất thường.

Hoạt động Threat Hunting có thể bao gồm phân tích log, metadata, lưu lượng mạng và các nguồn dữ liệu phù hợp nhằm phát hiện các mối nguy chưa được phát hiện bởi các cơ chế giám sát thông thường.

Kết quả cung cấp gồm các phát hiện, đánh giá nguy cơ, phạm vi ảnh hưởng và khuyến nghị xử lý.

5. Yêu cầu triển khai.

5.1. Yêu cầu khảo sát, sizing và triển khai

Nhà cung cấp có trách nhiệm khảo sát hiện trạng hệ thống CNTT của Bệnh viện, xác định phạm vi nguồn log, lưu lượng mạng và nhu cầu giám sát để thực hiện sizing các thành phần triển khai tại Bệnh viện.

Các thành phần phần cứng/phần mềm cần thiết để cung cấp dịch vụ MSS phải đáp ứng năng lực xử lý phù hợp với quy mô hệ thống thực tế và được nhà cung cấp đề xuất trong báo giá.

Nhà cung cấp chịu trách nhiệm cài đặt, cấu hình, tích hợp và đưa các thành phần thuộc phạm vi cung cấp vào vận hành.

5.2 Trách nhiệm phối hợp của Bệnh viện

Nhân sự quản trị hệ thống của Bệnh viện có trách nhiệm phối hợp với nhà

cung cấp trong việc cung cấp thông tin hiện trạng, cấu hình chuyển tiếp log từ các hệ thống thuộc phạm vi giám sát và thực hiện SPAN/TAP lưu lượng theo thiết kế được thống nhất.

6. Kết quả cung cấp dịch vụ:

Trong thời gian cung cấp dịch vụ, nhà cung cấp phải cung cấp tối thiểu:

- Hệ thống/ giao diện Dashboard phục vụ giám sát;
- Hệ thống quản lý và phối hợp xử lý sự cố/Trouble Ticket;
- Báo cáo an toàn thông tin định kỳ, tối thiểu gồm tình hình cảnh báo/sự cố, phân loại mức độ, các sự kiện đáng chú ý, tình hình xử lý, xu hướng nguy cơ và các khuyến nghị tăng cường an toàn thông tin;
- Báo cáo đột xuất khi phát sinh sự cố nghiêm trọng hoặc theo yêu cầu;
- Cảnh báo và thông tin phân tích đối với các sự kiện/sự cố thuộc phạm vi giám sát;
- Hỗ trợ phối hợp xử lý sự cố theo phạm vi hợp đồng;
- Báo cáo tổng kết và khuyến nghị tăng cường ATTT trong kỳ cung cấp dịch vụ.

7. Yêu cầu thông số cấu hình cơ bản thiết bị thu thập sự kiện, tối thiểu có:

EPS events per second	**Bandwidth (Mbps)**	**Specs Event Collector**			
		CPU	**RAM**	**Storage**	**Data transfer rate (MB/s)**
200	40	Intel Core i5-12400	16 GB	2TB	300

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

BỆNH VIỆN PHONG DA LIỄU TRUNG ƯƠNG QUY HÒA

Nguyễn Đăng Vinh