BỘ Y TẾ
**VIỆN SỐT RÉT - KÝ SINH TRÙNG CÔN TRÙNG TRUNG ƯƠNG**

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

Số: 776 /TB-VSR

*Hà Nội, ngày 03 tháng 7 năm 2026*

# YÊU CẦU BÁO GIÁ

**Cung cấp dịch vụ trang bị giải pháp và dịch vụ tư vấn đánh giá an toàn thông tin cho Bệnh viện Đặng Văn Ngữ thuộc Viện Sốt rét - Ký sinh trùng - Côn trùng Trung ương**

Kính gửi: Các công ty, đơn vị, nhà cung cấp dịch vụ trang bị giải pháp và dịch vụ tư vấn đánh giá an toàn thông tin

Hiện nay, Viện Sốt rét - Ký sinh trùng - Côn trùng Trung ương có nhu cầu tiếp nhận báo giá để tham khảo, xây dựng giá gói thầu, làm cơ sở tổ chức lựa chọn nhà thầu cung cấp dịch vụ trang bị giải pháp và dịch vụ tư vấn đánh giá an toàn thông tin cho Bệnh viện Đặng Văn Ngữ thuộc Viện Sốt rét- Ký sinh trùng-Côn trùng Trung ương. Nội dung cụ thể như sau:

**I. Thông tin của đơn vị yêu cầu báo giá:**

1. Đơn vị yêu cầu báo giá: Viện Sốt rét - Ký sinh trùng - Côn trùng Trung ương.

2. Cách thức tiếp nhận báo giá:

- 01 Bản cứng (có chữ ký, đóng dấu hợp pháp) gửi trực tiếp hoặc qua đường bưu điện; 01 file mềm gửi về địa chỉ: khdt.nimpe@gmail.com.

- Địa điểm nhận báo giá: Văn thư, Viện Sốt rét - Ký sinh trùng - Côn trùng Trung ương, địa chỉ: Số 34, đường Trung Văn, Phường Đại Mỗ, Thành phố Hà Nội.

3. Thời gian nhận báo giá từ 14 giờ 30 phút, ngày 03 tháng 7 năm 2026 đến trước 14 giờ 00 phút, ngày 14 tháng 7 năm 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 kể từ ngày báo giá.

**II. Nội dung yêu cầu báo giá:**

1. Hồ sơ báo giá hợp lệ: Báo giá phải có đầy đủ thông tin đơn vị báo giá, ngày, tháng, năm ký phát hành báo giá và thời gian hiệu lực của báo giá, đồng thời phải có ký xác nhận và đóng dấu theo quy định.

2. Báo giá đã bao gồm chi phí liên quan, thuế, phí, lệ phí của dịch vụ thực hiện và toàn bộ chi phí liên quan khác. Đơn vị báo giá thực hiện báo giá dịch vụ theo Mẫu báo giá tại **Phụ lục 01** kèm theo.

3. Danh mục chi tiết: **Phụ lục 2** kèm theo.

4. Địa điểm thực hiện dịch vụ: Bệnh viện Đặng Văn Ngữ thuộc Viện Sốt rét

- Ký sinh trùng - Côn trùng Trung ương; Địa chỉ: Số 245 Lương Thế Vinh, Phường Đại Mỗ, thành phố Hà Nội.

5. Nội dung khác (nếu có): Đơn vị báo giá gửi kèm theo các tài liệu chứng minh về căn cứ đề xuất giá chào và các tài liệu liên quan khác.

6. Thông tin chi tiết cần liên hệ: Bà Nguyễn Thị Phương Tiến, Phòng Kế hoạch tài chính, Bệnh viện Đặng Văn Ngữ; Số điện thoại: 0962889978.

Xin trân trọng cảm ơn./.

***Nơi nhận:***
- Như trên;
- Website của Viện, Bệnh viện (*để công khai*);
- Trang https://muasamcong.mpi.gov.vn;
- Lưu: VT, KHTH.

**VIỆN TRƯỞNG**

VIỆN SỐT RÉT KÝ SINH TRÙNG CÔN TRÙNG TRUNG ƯƠNG

Hoàng Đình Cảnh

## PHỤ LỤC 01: MẪU BÁO GIÁ

*(Kèm theo Thông báo số .... /TB-VSR ngày ... tháng ..... năm 2026 của Viện Sốt rét - Ký sinh trùng - Côn trùng Trung ương)*

**Mẫu báo giá:**

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

Tên đơn vị báo giá: .....
Địa chỉ: .....
Mã số thuế: .....
Số điện thoại liên hệ: ....
Email: .....

**BÁO GIÁ**

**Kính gửi: Viện Sốt rét-Ký sinh trùng-Côn trùng Trung ương**
Địa chỉ: 34 Trung Văn - Phường Đại Mỗ - Thành phố Hà Nội

Trên cơ sở yêu cầu báo giá của Viện Sốt rét-Ký sinh trùng-Côn trùng Trung ương tại Thông báo số ..... /TB-VSR ngày.....tháng....năm 2026, chúng tôi....[ghi tên, địa chỉ của hãng sản xuất, nhà cung cấp] báo giá cho hàng hóa như sau:

**1. Báo giá dịch vụ thực hiện:**

| TT | Danh mục dịch vụ | Mô tả dịch vụ | Đơn vị tính | Khối lượng | Đơn giá (VNĐ) | Chi phí liên quan, thuế, phí, lệ phí (nếu có) (VNĐ) | Thành tiền (VNĐ) | Địa điểm thực hiện dịch vụ |
|---|---|---|---|---|---|---|---|---|
| *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* |
| 1 | | | | | | | | |
| 2 | | | | | | | | |
| | **Tổng** | | | | | | | |

**3. Báo giá này có hiệu lực trong vòng:** .... ngày (Ghi cụ thể số ngày nhưng không *nhỏ hơn 90 ngày)*, kể từ ngày ..... tháng ..... năm 2026.

**4. Chúng tôi cam kết:**

- 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.
- Giá trị của dịch vụ nêu trong báo giá là phù hợp.
- Những thông tin nêu trong báo giá là trung thực.

....., ngày.... tháng....năm....

**Đại diện hợp pháp của hãng sản xuất, nhà cung cấp(*)**
(Ký tên, đóng dấu (nếu có))

**Ghi chú:**

(*) Người đại diện theo pháp luật hoặc người được người đại diện theo pháp luật ủy quyền phải ký tên, đóng dấu (nếu có). Trường hợp ủy quyền, phải gửi kèm theo giấy ủy quyền ký báo giá. Trường hợp liên danh tham gia báo giá, đại diện hợp pháp của tất cả các thành viên liên danh phải ký tên, đóng dấu (nếu có) vào báo giá.

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

# PHỤ LỤC 2: DANH MỤC CHI TIẾT

*(Kèm theo Thông báo số 776 /TB-VSR ngày 03 tháng 7 năm 2026 của Viện Sốt rét – Ký sinh trùng - Côn trùng Trung ương)*

## a. Danh mục, số lượng giải pháp an toàn thông tin cấp độ 2

| TT | Tên dịch vụ | Mục đích | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| 1 | Giải pháp Endpoint Security | **Bảo vệ 05 máy chủ của bệnh viện:** Ngăn chặn Ransomware (mã độc tống tiền) mã hóa hồ sơ bệnh án theo quy định. Bảo vệ an toàn dữ liệu trước các rủi ro an ninh mạng hiện hữu. | Gói/12 tháng | 1 |
| 2 | Tường lửa thông minh | Chặn lọc địa chỉ lừa đảo, độc hại: Tích hợp nguồn dữ liệu về mối nguy, tự động chặn các kết nối nguy hiểm<br>+ Phân vùng mạng Inside, Outside, DMZ…<br>+ Truy cập, kết nối từ xa an toàn thông qua VPN: Remote Access VPN và site-to-site VPN | Gói/12 tháng | 1 |
| 3 | Giải pháp tường lửa bảo vệ ứng dụng Web trên nền tảng đám mây | **Bảo vệ cổng đăng ký khám trực tuyến**: Ngăn chặn tin tặc tấn công vào website bệnh viện để đánh cắp thông tin cá nhân của bệnh nhân hoặc làm sập hệ thống đặt lịch, tránh gây hỗn loạn tại khu vực chờ khám. | Gói/12 tháng | 1 |
| 4 | Dịch vụ tư vấn, đánh giá cho ứng dụng | **Đảm bảo an toàn cho Ứng dụng/Website bệnh viện:** Phát hiện các lỗ hổng trong phần mềm quản lý bệnh viện (HIS, RIS, PACS...) Ngăn chặn tuyệt đối tình trạng rò rỉ hồ sơ bệnh án, dữ liệu cá nhân của bệnh nhân hoặc việc kẻ xấu giả mạo danh tính bác sĩ/quản trị viên để thực hiện các hành vi trái phép trên hệ thống. | Gói/lần | 1 |
| 5 | Dịch vụ tư vấn, đánh giá cho thiết bị (gói cho tối đa 10 thiết bị) | **Bảo vệ hạ tầng kết nối y tế:** Kiểm tra độ an toàn của tối đa 10 thiết bị mạng cốt lõi (Core Switch, Firewall, Server lưu trữ). Đảm bảo đường truyền dữ liệu giữa các khoa phòng luôn hoạt động thông suốt và không cho tin tặc xâm nhập. | Gói | 1 |
| 6 | Dịch vụ tư vấn, đánh giá đảm bảo an toàn hệ thống theo cấp độ | **Tuân thủ quy định pháp luật và chuẩn hóa:** Giúp bệnh viện hoàn thiện hồ sơ pháp lý, đáp ứng các tiêu chuẩn bảo mật của Bộ Y tế và Bộ Thông tin & Truyền thông. Xây dựng quy trình ứng phó sự cố chuyên nghiệp để bệnh viện không bị lúng túng khi gặp sự cố mạng. | Gói | 1 |

| TT | Tên dịch vụ | Mục đích | Đơn vị tính | Số lượng |
|---|---|---|---|---|
| | | Các giải pháp trên được khuyên cáo đáp ứng ATTT cấp độ theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ. | | |

**b. Yêu cầu kỹ thuật chung**

| TT | Hạng mục | Yêu cầu kỹ thuật |
|---|---|---|
| **I** | **Giải pháp Endpoint Security** | |
| | Bản quyền số lượng máy chủ bảo vệ | Bảo vệ 05 máy chủ vật lý |
| | Quản trị | Cloud hoặc OnPremise |
| | | Bảng điều khiển quản trị tập trung cho mọi thiết bị đầu cuối |
| | | Triển khai policy (chính sách), giám sát và phản hồi sự cố từ một nơi duy nhất |
| | Bảo vệ | **Diệt virus thế hệ mới (Next-Gen AV):** Phát hiện phần mềm độc hại bằng AI/ML, không phụ thuộc signature truyền thống |
| | | **Chống phần mềm độc hại:** Quét và loại bỏ virus, trojan, spyware, adware theo thời gian thực. |
| | | **Chống can thiệp:** Bảo vệ phần mềm đại diện (agent) khỏi việc bị vô hiệu hóa hoặc gỡ cài đặt trái phép. |
| | | **Giảm thiểu Ransomware:** Phát hiện, chặn các hành vi mã hóa bất thường và tự động khôi phục dữ liệu. |
| | | **Tường lửa (Firewall):** Tường lửa tích hợp giúp kiểm soát kết nối mạng vào/ra dựa trên các quy tắc (rule). |
| | Quét và phát hiện | **Local Scan:** Quét phần mềm độc hại trực tiếp trên thiết bị đầu cuối mà không cần kết nối tới máy chủ bảo mật. |
| | | **Hybrid Scan:** Kết hợp linh hoạt giữa Quét cục bộ và Quét tập trung tùy theo trạng thái kết nối mạng. |
| | | **Advanced Anti-Exploit:** Ngăn chặn các kỹ thuật khai thác lỗ hổng trên trình duyệt, ứng dụng văn phòng, trình đọc PDF và nhân hệ điều hành (kernel). |
| | | **Advanced Threat Control (ATC)** Phân tích hành vi của các tiến trình theo thời gian thực để phát hiện các mối đe dọa mới chưa có dấu hiệu nhận diện. |
| | Bảo vệ mạng | **Content Control** Kiểm soát truy cập web, ứng dụng theo danh mục và lịch trình |
| | | **Anti-Phishing** Chặn website giả mạo, lừa đảo theo thời gian thực |
| | | **Web Traffic Scan** Kiểm tra lưu lượng HTTP/HTTPS, phát hiện mối đe dọa ẩn trong traffic |

| TT | Hạng mục | Yêu cầu kỹ thuật |
|---|---|---|
| | | **Network Attack Defense** Phát hiện và chặn tấn công mạng, lateral movement, C2C |
| **II** | **Tường lửa thông minh** | |
| | Số lượng thiết bị cần lắp đặt | 01 |
| | Yêu cầu chung | Thiết bị được sản xuất trong nước, có minh chứng sở hữu trí tuệ, cung cấp đầy dủ giây tờ chứng minh xuất xứ, chứng nhận xuất xưởng trong nước |
| | | Sản phẩm phải được cấp phép sử dụng mật mã dân sự do Ban Cơ yếu chính phủ cấp |
| | | Sản phẩm phải được cấp phép cung cấp trên thị trường theo yêu cầu về giấy phép an toàn thông tin |
| | | Nhà thầu cung cấp đầy đủ tài liệu hướng dẫn sử dụng sản phẩm bằng tiếng Việt |
| | Tổng số phần cứng | Yêu cầu tối thiểu với thiết bị tường lửa:<br>+ Mới 100%<br>+ Nguồn điện: 220V, 50-60Hz<br>+ Tối thiểu 5 cổng mạng: 5 x GbE RJ45, tốc độ hỗ trợ tối đa: 1Gbps<br>+ Có tối thiểu 1 cổng quản trị RJ45 và 2 cổng USB 2.0<br>+ Power: 36W Power Adapter hoặc 40W Power Adapter<br>+ Kiểu dáng: Desktop hoặc 1U 19" Rackmount |
| | Thông lượng | - Firewall Throughput: 6 Gbps<br>- Threat Prevention Throughput: 1.5 Gbps<br>- IPS Throughput: 2.5 Gbps<br>- IPSec VPN Throughput: 1.5 Gbps<br>- Hỗ trợ tối thiểu 200 phiên VPN đồng thời.<br>- Hỗ trợ tối thiểu từ 300 đến 500 thiết bị kết nối đồng thời. |
| | Cấu hình mạng | Hỗ trợ cấu hình các giao diện mạng: Cho phép cấu hình từng Port, thiết đặt giao thức mạng, địa chỉ, cơ chế cấp phát IP,…. |
| | | Hỗ trợ định tuyến tĩnh theo Ipv4, Ipv6 |
| | | Hỗ trợ cấu hình phân giải tên miền (DNS) cho các địa chỉ nội bộ. |
| | | Hỗ trợ quản lý và giám sát thông tin địa chỉ IP của các thiết bị trong mạng |
| | | Hỗ trợ các giao thức định tuyến động OSPF |
| | | Hỗ trợ VLAN 802.1Q phục vụ phân vùng mạng. |
| | Tường lửa | Hỗ trợ cấu hình Port Forwarding, NAT và các chính sách kiểm soát lưu lượng mạng |
| | | Tích hợp chức năng phát hiện và ngăn chặn xâm nhập (IDS/IPS) |
| | | Truy cập, kết nối từ xa an toàn thông qua VPN: Remote Access VPN và site-to-site VPN |

| TT | Hạng mục | Yêu cầu kỹ thuật |
|---|---|---|
| | Bảo vệ an toàn mạng | Hỗ trợ phát hiện và ngăn chặn truy cập tới các địa chỉ IP hoặc tên miền (Domain) độc hại |
| | Giám sát và quản trị | Hỗ trợ xuất nhật ký hệ thống theo chuẩn Syslog. |
| | | Hỗ trợ giao thức SNMP phục vụ giám sát trạng thái và hiệu năng thiết bị |
| **III** | **Giải pháp tường lửa bảo vệ ứng dụng Web trên nền tảng đám mây** | |
| | Số lượng tên miền (domain) bảo vệ | 01 |
| | Yêu cầu chung | Nhà thầu phải cung cấp đầy đủ tài liệu hướng dẫn sử dụng giải pháp WAF bằng tiếng Việt |
| | | Nhà cung cấp phải cam kết mức độ sẵn sàng của hạ tầng dịch vụ (SLA uptime) tối thiểu đạt 99.95% |
| | | Nhà cung cấp phải cam kết hỗ trợ điện thoại, chat, email và ticket 16/7 |
| | | Giải pháp WAF phải hỗ trợ IPv6 |
| | | Giải pháp phải được thiết kế, nghiên cứu và phát triển bởi doanh nghiệp Việt Nam, trong đó doanh nghiệp trong nước làm chủ công nghệ lõi, có đội ngũ kỹ thuật và trung tâm hỗ trợ đặt tại Việt Nam, đảm bảo khả năng bảo trì, cập nhật và xử lý sự cố trong nước. |
| | Các tính năng WAF | WAF cung cấp khả năng chống các dạng tấn công vào điểm yếu của ứng dụng web theo OWASP |
| | | Giải pháp WAF có khả năng chống tấn công vào lỗ hổng của framework, webserver, công nghệ web (1-day, 0-day) |
| | | Giải pháp phải cho phép cấu hình chế độ OFF/ Detect only/ ON WAF cho website |
| | | Giải pháp phải hỗ trợ tính năng quản lý luật riêng và tùy chỉnh theo từng domain |
| | Tính năng chống tấn công DDOS | WAF khả năng chống các cuộc tấn công DDoS Layer 7 tối thiểu bao gồm: HTTP Flood, Slow attack (Slow POST, Slowloris) |
| | | WAF cung cấp khả năng giới hạn tần suất truy cập từ mỗi IP nguồn (theo số lượng request, số lượng connection) |
| | | WAF phải có quản lý danh sách IP Blacklist/Whitelist |
| | | Giải pháp hỗ trợ tính năng ngăn chặn bot với cookie challenge |
| | | Lưu lượng sạch bảo vệ đạt tối thiểu 500 RPS |
| | Giao diện quản trị | Giải pháp WAF phải có giao diện giám sát băng thông truy cập tối thiểu bao gồm các thông tin: BPS, RPS, CPS |
| | | Giải pháp WAF phải có giao diện giám sát sự kiện tấn công (WAF, DDoS L7) |
| | Cảnh báo và báo cáo | Giải pháp có khả năng cung cấp cảnh báo các đợt tấn công DDoS tới website được bảo vệ thông qua Email |

| TT | Hạng mục | Yêu cầu kỹ thuật |
|---|---|---|
| | | Giải pháp phải hỗ trợ tự động gửi báo cáo định kỳ |
| **IV** | **Dịch vụ tư vấn, đánh giá cho ứng dụng** | |
| | Số lượng ứng dụng cần đánh giá | Các ứng dụng gồm (HIS, RIS, PACS, EMR, phần mềm quản lý điều hành, mobile app) |
| | Tiêu chí chung | Sử dụng tối thiểu một trong các công cụ thương mại cần có bản quyền hợp lệ khi sử dụng để triển khai dịch vụ: Burp Suite Professional, Nessus, Nexpose, IDA Pro, Hopper, ... |
| | | Áp dụng các phương pháp đánh giá bảo mật theo các Framework của quốc tế như OWASP Testing guide, PTES, OSSTMM, NIST và thể hiện rõ phương pháp thực hiện trong báo cáo. |
| | | Cam kết hỗ trợ, tư vấn xử lý các vấn đề bảo mật sau khi đã thực hiện và gửi báo cáo. |
| | Nội dung kiểm tra, đánh giá | **Kiểm tra, đánh giá ứng dụng web dựa trên các rủi ro phổ biến được đề xuất bởi OWASP Top 10, tối thiểu bao gồm các nội dung:** |
| | | - Quản lý xác thực: xoay quanh mục đích tránh các lỗ hổng gây mất tài khoản của người dùng |
| | | - Quản lý phiên đăng nhập: mục đích nhằm tránh các lỗ hổng chiếm quyền đăng nhập của người dùng |
| | | - Phân quyền: mục đích tránh các lỗ hổng cho phép người dùng có thể thực hiện các chức năng không đúng quyền hạn |
| | | - Tương tác với back-end: mục đích nhằm tránh các lỗ hổng gây thất thoát và ảnh hưởng ngoài mong muốn đối với các dữ liệu của hệ thống như cơ sở dữ liệu, file… |
| | | - Kiểm soát dữ liệu đầu vào: mục đích nhằm đảm bảo các dữ liệu đưa lên cho server xử lý không tồn tại các dữ liệu gây ảnh hưởng đến an toàn thông tin hệ thống |
| | | - Kiểm soát dữ liệu đầu ra: mục đích nhằm đảm bảo thông tin hiện ra cho người dùng không thể gây ảnh hưởng đến an toàn thông tin của người dùng |
| | | - Kiểm soát lỗ hổng 1-day của các thư viện, framework: mục đích kiểm tra sự tồn tại của các lỗ hổng đã được công bố trên các thư viện, framework đang được sử dụng. |
| | | **Thực hiện rà soát, đánh giá đầy đủ các nhóm lỗ hổng bảo mật phổ biến trên ứng dụng, tối thiểu bao gồm:** |
| | | - Broken Access Control (BAC) *(Lỗi kiểm soát truy cập)* |
| | | - Broken Authentication and Management *(Lỗi xác thực và quản lý phiên)* |
| | | - Broken Cryptography *(Lỗi mã hóa dữ liệu)* |
| | | - Client-Side Injection *(Chèn mã phía Client)* |
| | | - Cross-Site Request Forgery (CSRF) *(Giả mạo yêu cầu liên trang (CSRF)* |

| TT | Hạng mục | Yêu cầu kỹ thuật |
|---|---|---|
| | | - Cross-Site Scripting (XSS) *(Chèn tập lệnh liên trang (XSS))* |
| | | - External Behavior *(Hành vi không mong muốn bên ngoài)* |
| | | - Insecure Data Storage *(Lưu trữ dữ liệu không an toàn)* |
| | | - Insecure Data Transport *(Truyền tải dữ liệu không an toàn)* |
| | | - Insecure OS/Firmware *(Hệ điều hành/Firmware không an* toàn) |
| | | - Insufficient Security Configurability *(Cấu hình bảo mật không đầy đủ)* |
| | | - Lack of Binary *Hardening (Thiếu cơ chế tăng cường bảo mật tệp nhị phân)* |
| | | - Logical Issues *(Lỗi logic (nghiệp vụ))* |
| | | - Mobile Security Misconfiguration *(Cấu hình bảo mật di động không an toàn)* |
| | | - Network Security Misconfiguration *(Cấu hình bảo mật mạng không an toàn)* |
| | | - Privacy Concerns *(Các vấn đề về quyền riêng tư)* |
| | | - Sensitive Data Exposure *(Lộ dữ liệu nhạy cảm)* |
| | | - Server Security Misconfiguration *(Cấu hình bảo mật máy chủ không an toàn)* |
| | | - Server-Side Injection (Chèn mã phía máy chủ) |
| | | - Unvalidated Redirects and Forwards *(Chuyển hướng và chuyển tiếp không được xác thực)* |
| | | - Using Components with Known Vulnerabilities *(Sử dụng các thành phần có lỗ hổng đã biết)* |
| | Báo cáo bàn giao | Báo cáo kết quả đánh giá ATTT ứng dụng/website |
| | | Báo cáo khuyến nghị khắc phục lỗ hổng bảo mật mức cao cho ứng dụng |
| **V** | **Dịch vụ tư vấn, đánh giá cho thiết bị (gói cho tối đa 10 thiết bị)** | |
| | Tiêu chí chung | Sử dụng tối thiểu một trong các công cụ thương mại cần có bản quyền hợp lệ khi sử dụng để triển khai dịch vụ: Burp Suite Professional, Nessus, Nexpose, IDA Pro, Hopper, ... |
| | | Cam kết hỗ trợ, tư vấn xử lý các vấn đề bảo mật sau khi đã thực hiện và gửi báo cáo. |
| | Công việc thực hiện | **Thực hiện thu thập thông tin cấu hình của các thành phần trong hệ thống, các thông tin như:**<br>- Cài đặt bản vá, cập nhật phiên bản<br>- Các thiết lập chính sách tài khoản<br>- Chính sách quản trị<br>- Chính sách truy cập.<br>- Chính sách thiết lập cấu hình |

| TT | Hạng mục | Yêu cầu kỹ thuật |
|---|---|---|
| | | Sử dụng công cụ chuyên dụng để rà quét các mục tiêu đã đã chỉ định, từ đó thực hiện rà quét để tìm kiếm các lỗ hổng tồn tại trong hệ thống. |
| | | Báo cáo các lỗ hổng phát hiện được trong quá trình đánh giá. |
| | | Báo cáo khuyến nghị khắc phục lỗ hổng bảo mật mức cao cho ứng dụng. |
| **VI** | **Dịch vụ tư vấn, đánh giá đảm bảo an toàn hệ thống theo cấp độ** | |
| | Phạm vi thực hiện | **Khảo sát hiện trạng hệ thống, hạ tầng:**<br>- Khảo sát tổng thể hệ thống<br>- Thông tin hạ tầng, thiết bị<br>- Thông tin dịch vụ, ứng dụng<br>- Hệ thống bảo mật hiện có<br>- Thông tin về chính sách, tổ chức bộ máy, hệ thống |
| | | **Đánh giá các quy trình, chính sách, quy định an toàn thông tin của tổ chức đáp ứng các yêu cầu về quản lý theo Tiêu chuẩn TCVN 11930:2017, gồm các nội dung:**<br>- Thiết lập chính sách an toàn thông tin<br>- Quy định về tổ chức, đơn vị bảo đảm an toàn thông tin<br>- Quản lý thiết kế, xây dựng hệ thống thông tin<br>- Quản lý vận hành hệ thống thông tin |
| | | **Đánh giá hệ thống hạ tầng công nghệ thông tin của tổ chức đáp ứng các yêu cầu về kỹ thuật theo Tiêu chuẩn TCVN 11930:2017, gồm các nội dung:**<br>- Đánh giá an toàn mạng<br>- Đánh giá an toàn máy chủ<br>- Đánh giá an toàn ứng dụng<br>- Đánh giá an toàn dữ liệu |
| | | **Tư vấn, đề xuất phương án:**<br>- Đưa ra báo cáo các vấn đề còn tồn tại, những điểm chưa đáp ứng yêu cầu của hệ thống thông tin cấp độ<br>- Đề xuất các phương án khắc phục cho đơn vị |
| | | **Xây dựng và hoàn thiện bộ hồ sơ đề xuất cấp độ cho chủ đầu tư** |

*Hà Nội, ngày 03 tháng 7 năm 2026*

**VIỆN TRƯỞNG**

VIỆN SỐT RÉT KÝ SINH TRÙNG CÔN TRÙNG TRUNG ƯƠNG

Hoàng Đình Cảnh