

Số: 723/TM-VAMC

Hà Nội, ngày 24 tháng 4 năm 2026

## THƯ MỜI

**Tham gia chào giá dịch vụ kiểm tra, đánh giá công tác đảm bảo an ninh, an toàn thông tin cho hệ thống CNTT tại VAMC năm 2026**

**Kính gửi: Các Công ty/đơn vị**

Công ty TNHH MTV Quản lý tài sản của các tổ chức tín dụng Việt Nam (VAMC) đang có nhu cầu kiểm tra, đánh giá công tác đảm bảo an ninh, an toàn thông tin cho hệ thống CNTT.

VAMC trân trọng kính mời Quý Công ty/đơn vị tham gia chào giá dịch vụ kiểm tra, đánh giá công tác đảm bảo an ninh, an toàn thông tin cho hệ thống CNTT tại VAMC năm 2026 với các nội dung sau:

### I. Mục đích

- Kiểm tra, rà soát cấu hình các thiết bị mạng, thiết bị bảo mật và hệ thống máy chủ theo các tiêu chuẩn và Quy định của NHNN.
- Phát hiện kịp thời các lỗ hổng bảo mật, điểm yếu kỹ thuật và nguy cơ mất an toàn thông tin (bao gồm rủi ro từ bên trong và tấn công từ bên ngoài).
- Đánh giá mức độ tuân thủ và hiệu quả của hạ tầng CNTT hiện tại so với cấp độ 2 an toàn thông tin.
- Đề xuất các biện pháp khắc phục, tối ưu cấu hình và nâng cao năng lực bảo vệ, đảm bảo tính liên tục vận hành và tuân thủ pháp luật.

### II. Phạm vi đánh giá

Kế hoạch áp dụng cho toàn bộ hạ tầng CNTT cốt lõi tại VAMC, bao gồm:

STT	Hệ thống	Số lượng	Mô tả
1	Switch Core Aruba 6300	01 cặp	Thiết bị chuyển mạch lõi hệ thống
2	Switch Aruba 2930	01 cặp	Thiết bị Switch kết nối máy chủ
3	Firewall Check Point 6200	01 cặp	Firewall bảo vệ kết nối vùng máy chủ nội bộ
4	Firewall SonicWall NSA 4650	01 cặp	Firewall VPN và internet
5	Máy chủ vật lý	02	Máy chủ chạy nền tảng ảo hóa
6	Máy chủ ảo	~ 40 máy	Các hệ thống ứng dụng nội bộ
7	Switch Layer 2 các tầng	12	Switch kết nối máy client



*Handwritten signature*

### III. Phạm vi nội dung công việc đánh giá

Kiểm tra được thực hiện theo 4 nhóm nội dung chính, kết hợp đánh giá cấu hình (Configuration Review), kiểm tra bảo mật (Security Audit) và thử nghiệm xâm nhập (Penetration Testing) theo khoản 1 điều 61 Quy chế “*Quản lý, sử dụng và an toàn hệ thống Công nghệ thông tin của Công ty Quản lý tài sản*”

#### 1. Rà soát cấu hình thiết bị mạng

- Kiểm tra phiên bản firmware và bản vá bảo mật
- Kiểm tra cấu hình VLAN, routing và ACL.
- Kiểm tra các cơ chế bảo vệ mạng: Port Security, DHCP Snooping...
- Kiểm tra cấu hình quản trị thiết bị (SSH, SNMP, Syslog).

#### 2. Rà soát cấu hình firewall

- Kiểm tra rule firewall, chính sách NAT.
- Kiểm tra hệ thống phòng chống xâm nhập (IPS).
- Kiểm tra cấu hình VPN và các cơ chế bảo vệ truy cập.
- Kiểm tra logging, cảnh báo và cơ chế dự phòng HA.

#### 3. Kiểm tra hệ thống máy chủ và nền tảng ảo hóa

- Kiểm tra phiên bản hệ điều hành và bản vá bảo mật.
- Kiểm tra phân quyền quản trị hệ thống.
- Kiểm tra cấu hình mạng của máy chủ ảo.
- Kiểm tra snapshot và cơ chế sao lưu – phục hồi dữ liệu (Veeam backup).
- Đánh giá tuân thủ quy trình vận hành và bảo mật theo Quy chế.

#### 4. Dò quét lỗ hổng bảo mật

- Sử dụng các công cụ chuyên dụng như Nmap, Nessus/OpenVAS... thực hiện quét lỗ hổng, phát hiện dịch vụ có nguy cơ bị tấn công cao và mô tả tấn công thực tế (theo phương pháp OWASP, PTES).

- Đánh giá rủi ro và tác động tiềm ẩn

### IV. Kết quả và thời gian thực hiện

- Báo cáo đánh giá an toàn thông tin hệ thống CNTT chi tiết (bao gồm mức độ rủi ro theo thang điểm và so sánh với tiêu chuẩn).

- Danh sách đầy đủ các lỗ hổng bảo mật, điểm yếu đã phát hiện (phân loại theo mức độ nghiêm trọng Critical/High/Medium/Low).

- Đề xuất cụ thể các biện pháp khắc phục kỹ thuật, tối ưu cấu hình và nâng cấp hạ tầng.

- Khuyến nghị dài hạn nhằm nâng cao mức độ bảo vệ an toàn thông tin, đảm bảo tuân thủ pháp luật và sẵn sàng cho các cuộc kiểm tra NHNN.

- Thời gian thực hiện: Dự kiến trong quý II/2026 (thời lượng khoảng 4-6 tuần, không ảnh hưởng hoạt động kinh doanh).

#### V. Yêu cầu chào giá

a) Giá chào là giá bao gồm VAT, các khoản chi phí phát sinh liên quan đến việc kiểm tra, đánh giá công tác đảm bảo an ninh, an toàn thông tin cho hệ thống CNTT tại VAMC năm 2026 và các chi phí cần thiết khác (nếu có).

c) Hồ sơ gửi kèm bản chào giá:

- Giấy phép hoạt động an toàn thông tin, an ninh mạng theo quy định pháp luật.

- Nhân sự đề xuất và chứng chỉ quốc tế (ISO/IEC 27001, chứng chỉ Pentest, v.v.) của nhân sự.

- Bản đề xuất thời gian, tiến độ thực hiện dự kiến (có tổng thời gian, tiến độ thực hiện toàn bộ các công việc và chi tiết đối với từng công việc) phù hợp với thực tiễn hạ tầng hiện tại của VAMC, tuân thủ nghiêm ngặt các quy định pháp luật và tiêu chuẩn an toàn thông tin quốc tế, nhằm đảm bảo tính khả thi và hiệu quả cao nhất.

Chào giá gửi về VAMC theo địa chỉ sau:

- Hình thức gửi chào giá: Bản cứng có dấu đỏ gửi trực tiếp hoặc theo đường bưu điện.

- Nơi nhận: Ban Hành chính - Nhân sự, Công ty TNHH MTV Quản lý tài sản của các tổ chức tín dụng Việt Nam.

- Địa chỉ nhận: 300 Tôn Đức Thắng, Phường Ô Chợ Dừa, Hà Nội.

- Thời gian nhận: đến hết ngày 05/5/2026 (trong giờ hành chính).

- Điện thoại liên hệ: 0982 621 534.

Trân trọng./.

Nơi nhận:

- Như kính gửi;
- Lưu HCNS.



*Dặng Đình Thích*

