

# **YÊU CẦU VỀ KỸ THUẬT**

## **Mục 1. Yêu cầu về kỹ thuật**

### **1.1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu**

- Bên mời thầu: Trung tâm 386/BTL86.
- Tên gói thầu: Nâng cấp phần mềm tìm kiếm thông tin.
- Nguồn vốn: Ngân sách nhà nước năm 2026.
- Thời gian tổ chức lựa chọn nhà thầu: 45 ngày.
- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý II năm 2026.
- Hình thức lựa chọn nhà thầu: Đấu thầu rộng rãi qua mạng.
- Phương thức lựa chọn nhà thầu: Một giai đoạn một túi hồ sơ.
- Loại hợp đồng: Trọn gói.
- Thời gian thực hiện hợp đồng: 75 ngày.

### **1.2. Yêu cầu về kỹ thuật**

Tóm tắt thông số kỹ thuật của hàng hóa phải tuân thủ các thông số kỹ thuật và các tiêu chuẩn sau đây:

#### **1.2.1 Các Yêu cầu chung**

##### **1.2.1.1. Tiêu chuẩn kỹ thuật thông tin**

Hệ thống đáp ứng danh mục tiêu chuẩn kỹ thuật CNTT áp dụng chủ yếu dựa trên danh mục ban hành kèm thông tư 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ TT&TT về Ban hành danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước.

##### **1.2.1.2. Yêu cầu về an toàn thông tin đối với phần mềm**

Các yêu cầu cơ bản đảm bảo an toàn Hệ thống:

- Có thiết lập yêu cầu bảo đảm mật khẩu trên ứng dụng đủ độ phức tạp cần thiết để hạn chế tấn công dò quét mật khẩu; các thông tin xác thực phải được lưu trữ dưới dạng mã hóa;
- Có thiết lập yêu cầu ghi nhật ký truy cập, lỗi phát sinh;
- Người sử dụng hệ thống phải được cấp quyền đối với đối tượng người dùng cụ thể.

**1.2.1.3 Yêu cầu về tích tương thích và tích hợp:** Phần mềm nâng cấp phải hoạt động tốt trên nền tảng hiện có và tương thích với hệ thống hoạt động.

##### **1.2.1.4. Yêu cầu về thiết kế phần mềm**

- Giao diện được trình bày khoa học, hợp lý và đảm bảo mỹ thuật hài hòa với mục đích, tuân thủ các chuẩn về truy cập thông tin.

- Tương thích với các trình duyệt Web thông dụng.

### **1.2.1.5 Yêu cầu đào tạo, chuyển giao công nghệ và hỗ trợ kỹ thuật**

#### **a. Yêu cầu chuyển giao**

Để đảm bảo cho các cán bộ kỹ thuật được giao có thể vận hành một cách hiệu quả hệ thống, nhà thầu tổ chức tập huấn, đào tạo; trong quá trình tập huấn chuyển giao hệ thống đề xuất nhà thầu sẽ trao đổi và chuyển giao những kinh nghiệm đã đạt được trong quá trình triển khai một cách thống nhất và có trách nhiệm để cán bộ của phụ trách hệ thống có thể độc lập trong quá trình vận hành hệ thống mới của mình.

#### **b. Hỗ trợ kỹ thuật**

- Nhà thầu phải có quy trình hỗ trợ kỹ thuật:

+ Thời gian phản hồi và xác định lỗi: Trong vòng tối đa 02 giờ làm việc kể từ thời điểm nhận được thông báo hỗ trợ.

+ Thời gian đáp ứng: Tùy vào các lỗi kỹ thuật được xác định nhà thầu có cơ chế đưa ra thời gian xử lý hợp lý, phân loại lỗi theo mức độ, thời gian xử lý lỗi tối đa 02 ngày; Cam kết có mặt tại địa điểm thông báo trong vòng tối đa 48 giờ làm việc kể từ thời điểm nhận được thông báo đối với các trường hợp yêu cầu xử lý tại địa điểm triển khai (có mặt tại nơi thông báo, bắt đầu thực hiện hành động hỗ trợ);

- Thời gian hỗ trợ kỹ thuật được tính từ khi ký biên bản bàn giao và nghiệm thu hàng hóa.

### **1.2.1.6. Yêu cầu bảo hành, bảo trì**

Đối với các hạng mục phần mềm nội bộ nhà thầu cung cấp, nhà thầu phải chịu trách nhiệm bảo hành với các điều kiện sau:

- Tất cả các lỗi của phần mềm.

- Thời gian bảo hành được tính kể từ khi ký biên bản bàn giao và nghiệm thu hàng hóa.

- Phần mềm phải bảo hành trong vòng 24 tháng kể từ ngày ký biên bản nghiệm thu.

- Phần mềm phải được hỗ trợ về mặt kỹ thuật lập trình và triển khai trong thời gian 24 tháng, tính từ ngày hai bên ký biên bản nghiệm thu thanh lý hợp đồng.

- Phương tiện hỗ trợ thông qua: fax, thư tín điện tử, điện thoại, internet, chuyên phát bưu phẩm và hỗ trợ tại chỗ (onsite).

- Phần mềm phải được cam kết hỗ trợ bảo trì sản phẩm ứng dụng sau khi kết thúc giai đoạn bảo hành nếu chủ đầu tư có nhu cầu.

### **1.2.1.7. Yêu cầu cài đặt, cấu hình dịch vụ**

Dịch vụ được triển khai và bàn giao theo phương thức trọn gói. Vì vậy, nhà thầu đóng vai trò tích hợp dịch vụ, chủ trì để thực hiện lắp đặt, cài đặt, cấu hình, thiết lập tham số, tinh chỉnh theo đúng kiến trúc đảm bảo đáp ứng các yêu cầu.

### **1.2.1.8. Yêu cầu về bàn giao sản phẩm**

Nhà thầu chuyển giao các tài liệu hạng mục sau đây cho Chủ đầu tư:

- Mã nguồn của chương trình.
- Giấy chứng nhận bản quyền phần mềm phía nhà thầu.
- Các tài liệu hướng dẫn sử dụng, quản trị, hướng dẫn sử dụng hệ thống, tài liệu phân tích thiết kế hệ thống (tài liệu phải viết bằng tiếng Việt)

### **1.2.2. Yêu cầu về kỹ thuật chi tiết**

Phần mềm được triển khai dưới dạng ứng dụng web, gồm các chức năng chính sau:

#### a) Quản lý đơn vị

Theo dõi thông tin đơn vị: lưu trữ và cập nhật thông tin cơ cấu đơn vị, các đơn vị thuộc quyền, các đơn vị liên quan.

#### b) Quản lý thông tin thiết bị mạng

Bao gồm kiểm tra trạng thái thiết bị, quản lý các thông tin về chủng loại, đơn vị sử dụng và các thông tin liên quan.

#### c) Quản lý tập luật

Thiết lập các tập luật thể hiện các logic trong môi trường mạng quân sự, phát hiện các kết nối bất thường dựa trên địa chỉ và cổng nguồn – đích.

#### d) Kết nối dữ liệu ClickHouse

Tích hợp và đồng bộ dữ liệu: Thiết lập kết nối trực tiếp với cơ sở dữ liệu ClickHouse, cho phép nhận, truyền và đồng bộ dữ liệu log từ nhiều nguồn như thiết bị mạng, firewall, IDS/IPS, endpoint, server ứng dụng... theo thời gian thực.

#### e) Quản lý log

Chức năng quản lý các thông tin log được lưu trữ, gom nhóm, tìm kiếm theo khoảng gian. Hệ thống thực hiện thu thập các luồng dữ liệu log từ thiết bị mạng, thực hiện chuẩn hóa để phân loại, gán mức độ ưu tiên, rủi ro.

#### f) Quản lý sự kiện

Khi xuất hiện cảnh báo, các thông tin được lưu trữ lại, giúp người sử dụng có thể truy vết được luồng thông tin gây ra cảnh báo. Chức năng này cung cấp khả năng tìm kiếm, lọc các chi tiết của các cảnh báo đã xuất hiện.

g) Dự đoán khả năng xảy ra sự cố bảo mật theo thời gian

Hệ thống kết hợp mô hình xác suất cũng như các mô hình AI nhằm tổng hợp các khả năng rủi ro đến các vị trí thiết bị mạng/máy chủ. Từ đó, phát hiện các nguy cơ có thể xảy ra, thông báo đến người quản trị kịp thời.

h) Trực quan hóa bằng sơ đồ timeline

Hệ thống dựa trên nguồn log được cấu hình tập trung, mô hình hóa và phân tích các chuỗi tấn công phức tạp một cách trực quan và dễ hiểu dựa trên các kỹ thuật AI.

i) Phát hiện, phân tích hành vi bất thường

Chức năng ứng dụng Deep-learning kết hợp AI cổ điển và phương pháp rule-based nhằm phát hiện, phân tích hiệu quả các hành vi bất thường với các chuỗi hành vi được thu thập từ các nguồn log trên các thiết bị mạng.

**Chức năng chi tiết của phần mềm cụ thể như sau:**

STT	Chức năng	Mô tả yêu cầu
1	Quản lý đơn vị	Thêm thông tin đơn vị
		Bổ sung, chỉnh sửa thông tin đơn vị
		Xóa thông tin đơn vị
		Tìm kiếm đơn vị
2	Quản lý thông tin thiết bị mạng	Theo dõi trạng thái kết nối thiết bị mạng
		Bổ sung thông tin thiết bị mạng
		Xóa thông tin thiết bị mạng
		Tìm kiếm thiết bị mạng
3	Quản lý tập luật	Thêm tập luật
		Bổ sung, chỉnh sửa thông tin tập luật
		Xóa/kích hoạt/vô hiệu hóa tập luật
		Tìm kiếm tập luật
4	Kết nối dữ liệu ClickHouse	Kiểm tra kết nối, thực hiện kết nối dữ liệu từ API của cơ sở dữ liệu lớn ClickHouse
5	Quản lý log	Lựa chọn nguồn log
		Lọc nguồn log theo thời gian
		Tìm kiếm log
		Xuất log ra file csv
6	Quản lý sự kiện	Lọc sự kiện theo loại sự kiện
		Lọc sự kiện theo thời gian
		Tìm kiếm sự kiện
		Xuất sự kiện ra file csv
7		Trích xuất đặc trưng rủi ro theo thời gian

	Dự đoán khả năng xảy ra sự cố bảo mật	Sử dụng thống kê, AI để dự đoán xác suất dấu hiệu bị tấn công
		Tổng hợp kết quả nhận định khả năng rủi ro
		Hiển thị cảnh báo, liệt kê thông tin các vị trí khả năng sự cố bảo mật cao.
8	Trực quan hóa bằng sơ đồ timeline	Lựa chọn khung thời gian, bộ lọc timeline
		Sử dụng mô hình học máy để dự đoán và diễn giải
		Trực quan hóa dòng log bằng biểu đồ
		Xuất báo cáo
9	Phát hiện, phân tích hành vi bất thường	Thu thập và làm sạch log từ các nguồn
		Chuẩn hóa, tạo hồ sơ chuỗi hành vi
		Trích xuất đặc trưng hành vi
		Đối chứng hành vi với danh sách tập luật
		Ghi nhận nhận định sơ bộ
		Gom nhóm các hành vi
		Phát hiện hành vi bất thường qua trí tuệ nhân tạo
		Kết luận chuỗi hành vi, lưu trữ kết luận

Phần mềm được xây dựng theo mô hình client-server, hoạt động trên nền tảng web, sử dụng các công nghệ:

- Back-end: Ngôn ngữ lập trình Python, framework Flask.
- Front-end: Framework Bootstrap.
- Dữ liệu lớn: ClickHouse.
- Trí tuệ nhân tạo: PyTorch.
- Hệ điều hành máy chủ: Linux.

### **1.3. Các yêu cầu khác**

Bản quyền: Bản quyền vĩnh viễn, sản xuất năm 2026.

#### **1.3.1 Phương án tổ chức, triển khai, thực hiện**

- Phương án cài đặt, triển khai, vận hành: Hệ thống sau khi được xây dựng sẽ triển khai kiểm thử, vận hành, cài đặt sử dụng tại Trung tâm 386/BTL86.

- Phương án kiểm thử các yêu cầu chức năng và phi chức năng của hệ thống: Khi nhà thầu thông báo là đã hoàn thành giai đoạn phát triển, các đơn vị cần tiến hành kiểm thử, kiểm tra an toàn thông tin để hoàn thiện phần mềm trước khi tiến hành nghiệm thu sản phẩm.

1.3.2 Cam kết của đơn vị phát triển về quá trình bảo hành và hỗ trợ kỹ thuật sau khi hệ thống đưa vào vận hành, khai thác.

- Thời gian bảo hành đối với phần mềm tối thiểu là 24 tháng kể từ ngày nghiệm thu bàn giao.

- Đơn vị triển khai dự án phải có trách nhiệm bảo hành sản phẩm khi có bất kỳ một đơn vị thụ hưởng nào báo hệ thống có lỗi hoặc không đáp ứng yêu cầu và

phải có trách nhiệm cập nhật bản vá lỗi cho tất cả các đơn vị thụ hưởng khác trong thời gian bảo hành. Một khi ứng dụng có sự điều chỉnh mã nguồn do khắc phục lỗi hoặc nâng cấp chức năng của phần mềm. Đơn vị triển khai phải bàn giao CD (2 bản có nội dung giống nhau) mã nguồn và các tài liệu có liên quan đến việc hiệu chỉnh phần mềm cho Chủ đầu tư.

- Thời gian xử lý lỗi tối đa: Trong vòng 02 ngày khi Bên A thông báo cho bên B và xác định được lỗi và tùy với mức phân loại lỗi có thời gian xử lý phù hợp.

## **Mục 2. Kiểm tra và thử nghiệm**

1. Kiểm tra, thử nghiệm sẽ được tiến hành khi hàng đến địa điểm bàn giao theo yêu cầu của E-HSMT.

2. Cách thức tiến hành kiểm tra, thử nghiệm: Bên mời thầu sẽ trực tiếp kiểm tra, thử nghiệm hàng hóa với sự chứng kiến của nhà thầu. Dịch vụ phải được vận hành thử theo quy định tại Phụ lục II ban hành kèm theo Thông tư số 24/2020/TT-BTTTT ngày 09/9/2020 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về công tác triển khai, giám sát công tác triển khai và nghiệm thu dự án đầu tư ứng dụng công nghệ thông tin sử dụng nguồn vốn ngân sách nhà nước.

3. Hàng hóa phải được giám định chất lượng, kiểm tra an toàn thông tin đạt yêu cầu. Giám định chất lượng, kiểm tra, an toàn thông tin của hàng hóa theo quy định của Bộ Quốc phòng.

4. Trường hợp hàng hóa không phù hợp với đặc tính kỹ thuật theo hợp đồng thì Bên mời thầu có quyền từ chối và nhà thầu phải có trách nhiệm thay thế hoặc tiến hành những điều chỉnh cần thiết để đáp ứng đúng các yêu cầu về đặc tính kỹ thuật. Trường hợp nhà thầu không có khả năng thay thế hay điều chỉnh hàng hóa không phù hợp, Bên mời thầu có quyền tổ chức việc thay thế hay điều chỉnh nếu thấy cần thiết, mọi rủi ro và chi phí liên quan do Nhà thầu chịu. Việc thực hiện kiểm tra, thử nghiệm hàng hóa của Bên mời thầu không dẫn đến miễn trừ nghĩa vụ bảo hành hay các nghĩa vụ khác theo hợp đồng của Nhà thầu.

