

Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

Yêu cầu về kỹ thuật bao gồm các nội dung cơ bản như sau:

Mục 1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

1.1. Thông tin dự án

1. Tên dự án: Nâng cấp phần mềm lập báo cáo công tác nghiên cứu phụ tải
2. Giá trị dự toán: 2.974.757.569 đồng (Bằng chữ: Hai tỷ, chín trăm bảy mươi bốn triệu, bảy trăm năm mươi bảy nghìn, năm trăm sáu mươi chín đồng)
3. Chủ đầu tư: Công ty Viễn thông điện lực và Công nghệ thông tin - Chi nhánh Tập đoàn Điện lực Việt Nam
4. Nguồn vốn: Vốn tự có của EVN
5. Thời gian thực hiện dự án:
 - Hoàn thành triển khai thí điểm: Tháng 8 năm 2026
 - Hoàn thành triển khai: Tháng 9 năm 2026
6. Phạm vi thực hiện:

Hệ thống gồm các chức năng tại bảng sau:

STT	Chức năng
1	Danh mục thông tin
2	Chức năng khai báo cấu hình
3	Chức năng nhận số liệu
4	Chức năng xem báo cáo

7. Phạm vi triển khai: Triển khai tập trung tại EVN
8. Địa điểm đầu tư: Tại Công ty Viễn thông điện lực và Công nghệ thông tin, Tòa nhà EVN, số 11 Cửa Bắc, Ba Đình, Hà Nội.

1.2. Thông tin gói thầu

1.2.1. Phạm vi công việc gói thầu

- Khảo sát thu thập thông tin và xây dựng Phương án triển khai kiểm tra, đánh giá ANM&ATTT
- Kiểm tra, đánh giá ANM&ATTT hệ thống gồm:
 - Đánh giá điểm yếu mã nguồn ứng dụng
 - Đánh giá điểm yếu thư viện
 - Đánh giá điểm yếu và kiểm thử xâm nhập API
 - Đánh giá điểm yếu và kiểm thử xâm nhập ứng dụng
 - Đánh giá điểm yếu và kiểm thử xâm nhập hạ tầng CNTT

- Tổng hợp và lập báo cáo đánh giá ANM&ATTT và khuyến nghị khắc phục các lỗ hổng
- Tái đánh giá ANM&ATTT và báo cáo tái đánh giá kết quả khắc phục lỗ hổng

1.2.2. Thời gian thực hiện gói thầu

100 ngày tính từ ngày hợp đồng có hiệu lực và Bên A có văn bản thông báo nhà thầu thực hiện hợp đồng đến ngày ký Biên bản nghiệm thu hợp đồng, trong đó:

- Thời gian khảo sát thu thập thông tin hệ thống: 07 ngày
- Thời gian đánh giá ANM&ATTT: 43 ngày
- Thời gian khắc phục lỗ hổng (nếu có): 30 ngày
- Thời gian tái đánh giá ANM&ATTT: 10 ngày
- Thời gian nghiệm thu hợp đồng: 10 ngày

Mục 2. Mục tiêu công việc:

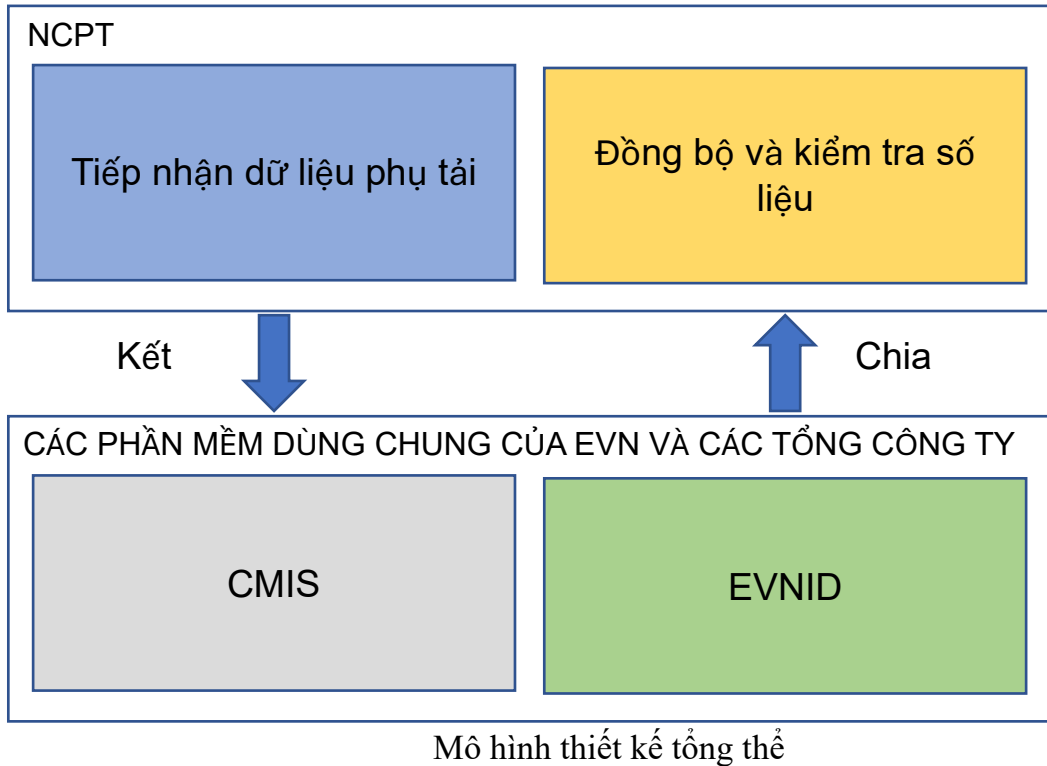
Đánh giá ANM&ATTT cho phần mềm lập báo cáo công tác nghiên cứu phụ tải nhằm phát hiện các lỗ hổng, điểm yếu của phần mềm, từ đó có giải pháp khắc phục lỗ hổng bảo mật nhằm ngăn chặn việc kẻ tấn công khai thác các lỗ hổng bảo mật đánh cắp dữ liệu, thay đổi hoặc mã hóa dữ liệu, chiếm quyền điều khiển hệ thống, gây tổn hại tới hệ thống CNTT của EVN.

Đánh giá ANM&ATTT nhằm đảm bảo hệ thống đủ điều kiện cho việc triển khai chính thức.

Sau đây là thiết kế của phần mềm lập báo cáo công tác nghiên cứu phụ tải

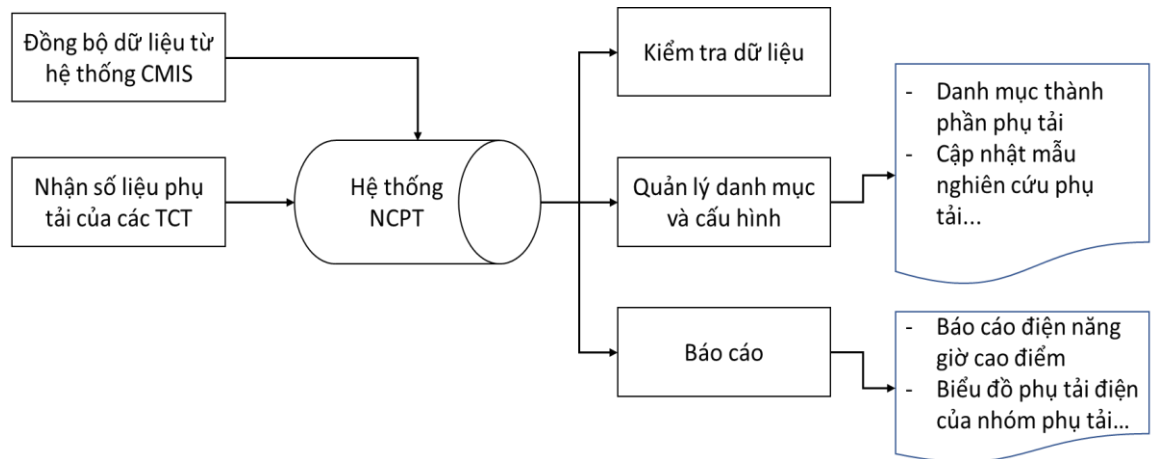
2.1. Thiết kế hệ thống phần mềm

2.1.1. Mô hình tổng quan

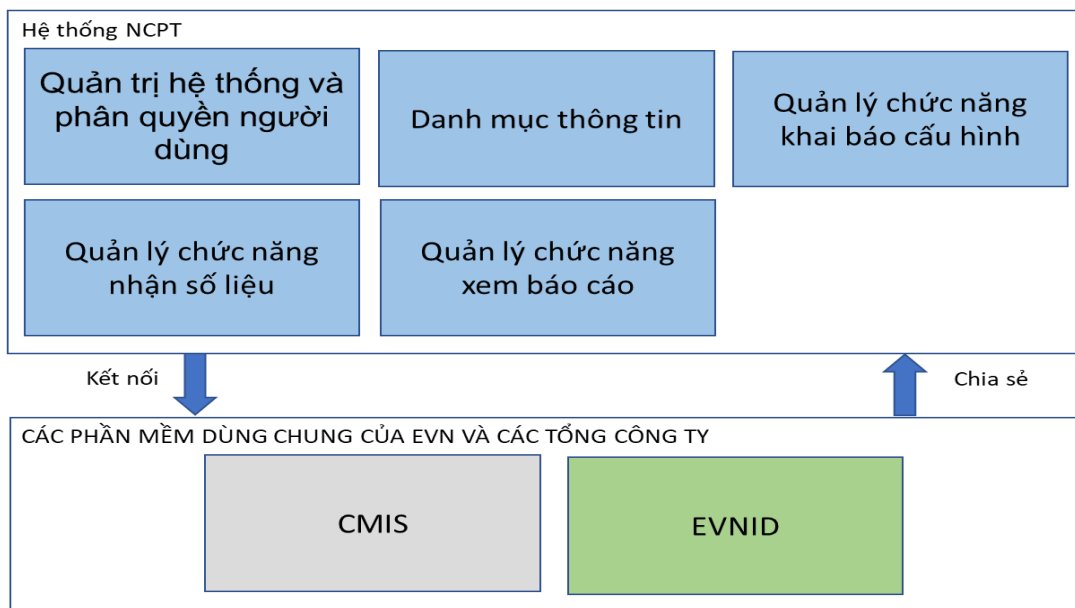


- Mô tả các thành phần
 - o Tiếp nhận dữ liệu phụ tải
 - Nhận dữ liệu từ các file excel để thể hiện trên các báo cáo cũng như biểu đồ
 - o Đồng bộ và kiểm tra số liệu:
 - Luồng đồng bộ nhận dữ liệu: Hệ thống sẽ đồng bộ các dữ liệu từ hệ thống CMIS của các tổng công ty.
 - Luồng đồng bộ gửi dữ liệu: Với dữ liệu mà hệ thống CMIS chưa có cần có để xử lý thì NCPT sẽ chia sẻ các dữ liệu được yêu cầu có trên hệ thống.
 - Kiểm tra số liệu: Với dữ liệu kết nối đồng bộ từ CMIS về NCPT sẽ kiểm tra độ chính xác số liệu được tiếp nhận.

2.1.2. Mô hình tổng thể hệ thống



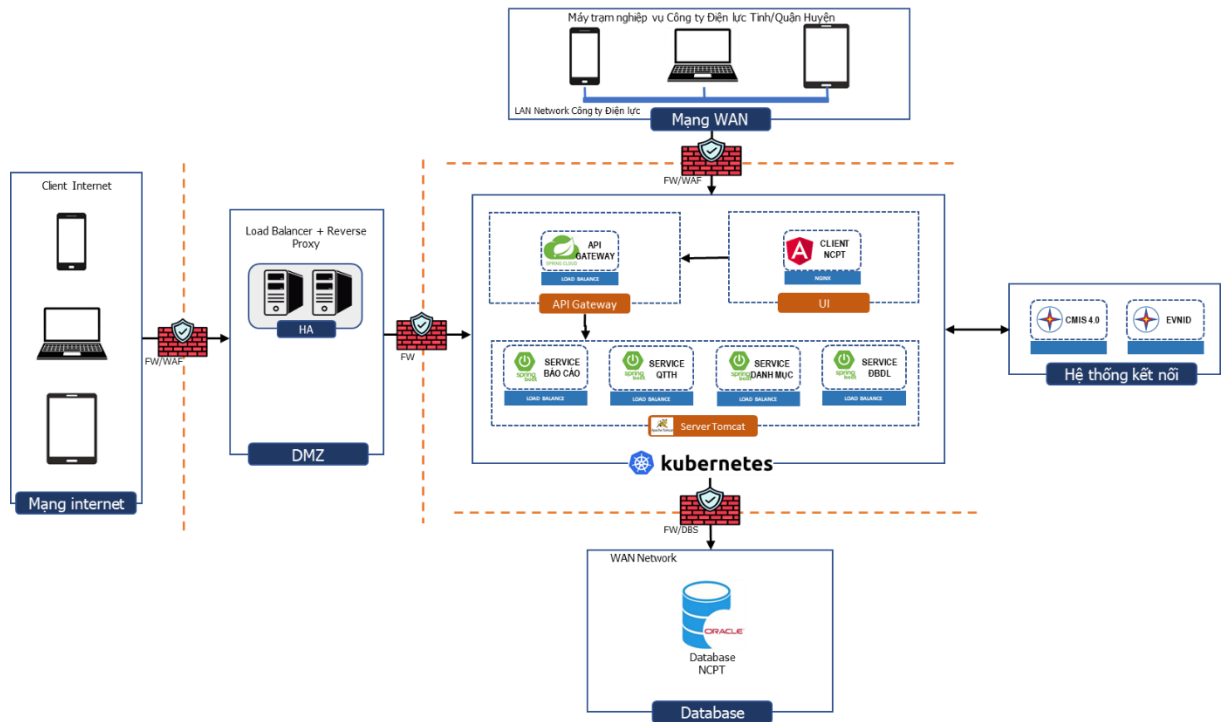
Sơ đồ liên kết NCPT với các phần mềm khác



- Hệ thống gồm các phân hệ:
 - Quản trị hệ thống và phân quyền người dùng: Phân hệ này được tận dụng, kế thừa lại từ các hệ thống sẵn có phân hệ Quản trị tập trung.
 - Danh mục thông tin: Quản lý các cấu hình danh mục dùng chung và riêng của các nghiệp vụ.
 - Quản lý chức năng khai báo cấu hình: Quản lý các cấu hình phục vụ các chức năng nghiệp vụ của hệ thống.
 - Quản lý chức năng nhận số liệu: Tiếp nhận, đồng bộ và kiểm tra số liệu phụ tải của các TCT.
 - Quản lý chức năng xem báo cáo: Xem các báo cáo, biểu đồ phụ tải.

• Mô hình kiến trúc phát triển ứng dụng

Kiến trúc phát triển ứng dụng được thiết kế như sau:



Mô hình kiến trúc ứng dụng

Mô tả các thành phần kiến trúc:

- Client Access
 - o Ứng dụng Web: Giao diện người dùng chạy trên các trình duyệt (Chrome, Firefox, Edge).
- Kết nối mạng:
 - o Client WAN: Truy cập nội bộ thông qua Firewall.
 - o Client Internet: Truy cập từ Internet thông qua WAF + Firewall.
- Lớp Bảo mật
 - o WAF (Web Application Firewall): Ngăn chặn tấn công DDoS, SQL Injection, XSS từ internet.
 - o Firewall: Kiểm soát truy cập, chỉ cho phép lưu lượng từ các nguồn tin cậy và cổng được định nghĩa.
- Load Balancer (F5)
 - o Phân phối tải (Load Balancing) giữa các instance của Spring Cloud Gateway.
 - o Thực hiện chuyển đổi dự phòng (Failover) để đảm bảo tính sẵn sàng cao.
 - o Xử lý mã hóa SSL/TLS termination.
- API Gateway (Nginx)
 - o Vai trò: Là điểm vào duy nhất cho tất cả các client, chịu trách nhiệm:
 - o Định tuyến (Routing): Định tuyến các request đến microservice backend phù hợp.
 - o Xác thực & Ủy quyền (Authentication & Authorization): Có thể tích hợp để kiểm tra JWT hoặc token.
 - o Rate Limiting: Giới hạn số request để bảo vệ backend service.

- Logging & Tracing: Ghi log và theo dõi request cho mục đích giám sát.
- Triển khai: Được triển khai thành cụm (cluster) trên các Server Tencent (Mango LAN) để đảm bảo khả năng chịu lỗi và mở rộng ngang.

- Microservices

Các service độc lập, được triển khai riêng biệt trên các server. Giao tiếp giữa các service sử dụng cơ chế Đồng bộ (REST API) hoặc Bất đồng bộ (thay thế Kafka bằng cơ chế đơn giản hơn như Database Polling hoặc Scheduled Tasks nếu cần).

- API Hệ thống: Quản lý phân quyền và quản trị hệ thống.
- API Danh mục: Quản lý danh mục, cấu hình.
- API Đồng bộ dữ liệu: Chịu trách nhiệm thu thập, đồng bộ hóa dữ liệu từ các nguồn nội bộ (LRS, CMIS) và bên ngoài.
- API Báo cáo: Thực hiện tất cả các nghiệp vụ phân tích, xử lý dữ liệu (phân tích biểu đồ, xu hướng, tăng trưởng) và cung cấp các loại báo cáo cho các cấp (TCT, EVN).

- Database: gồm các cơ sở dữ liệu lịch sử, quan hệ

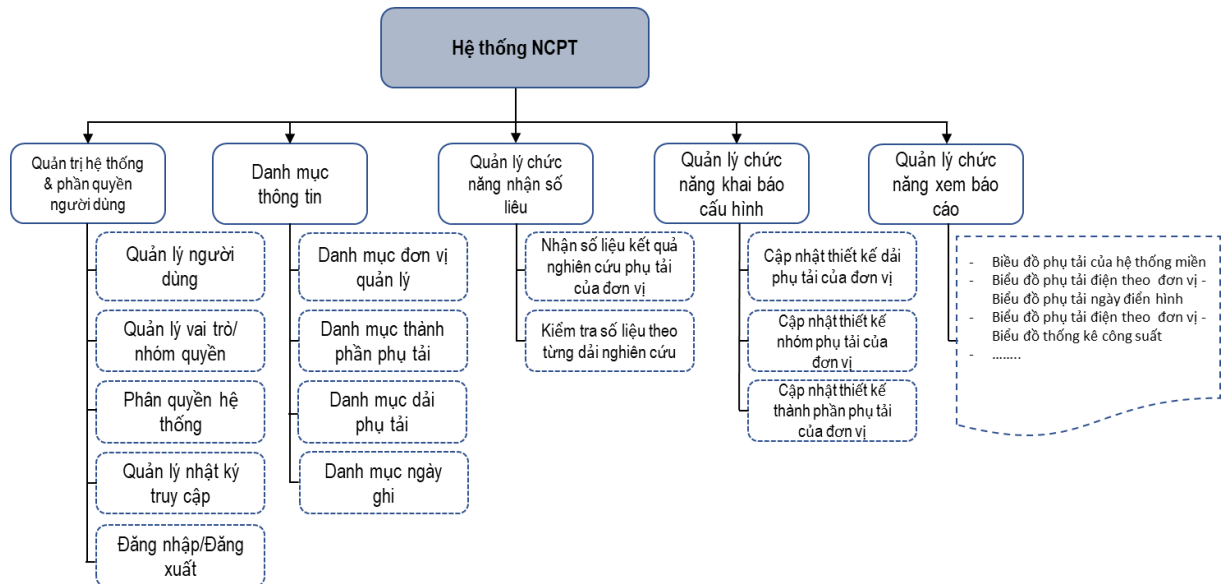
Mỗi microservice có cơ sở dữ liệu riêng biệt, đảm bảo nguyên tắc tách biệt trong kiến trúc microservices.

- DB Nghiên cứu phụ tải: Lưu trữ dữ liệu của quản lý người dùng, phân quyền, chức năng, danh mục và cấu hình hệ thống. Lưu trữ dữ liệu thô được thu thập và đồng bộ từ các nguồn và dữ liệu đã qua xử lý, kết quả phân tích, mẫu báo cáo và lịch sử xuất báo cáo.
- Triển khai: Các database được đặt trong Name WAN, trên các Server File DB và Server Host DB để đảm bảo hiệu năng và bảo mật.
- Cơ chế Đồng bộ (Thay thế Message Queue)
 - Cơ chế Đồng bộ trực tiếp: Sử dụng các API REST để đồng bộ dữ liệu giữa các service khi cần thiết.
- Utility Services
 - Các service tiện ích được gọi trực tiếp bởi các microservice thông qua REST API:
 - API EVNID: Cung cấp dịch vụ xác thực người dùng tập trung sử dụng tài khoản EVNID.
 - API CMIS: Cung cấp dữ liệu đồng bộ các tiêu chí báo cáo.

2.1.3. Phân tích và mô tả chức năng của phần mềm

a) Mô hình chức năng tổng thể

Hệ thống bao gồm các chức năng chính sau:



b) Phân tích và mô tả chức năng

- Bảng phân tích, mô tả chức năng

STT	Danh sách chức năng
I	Quản trị hệ thống và phân quyền người dùng
1.	Quản lý người dùng
2.	Đăng nhập, đăng xuất tài khoản
3.	Quản lý vai trò/nhóm quyền.
4.	Phân quyền hệ thống
5.	Đổi mật khẩu
6.	Quản lý nhật ký truy cập người dùng
II	Danh mục thông tin
1.	Danh mục đơn vị quản lý
2.	Danh mục nhóm thành phần phụ tải
3.	Danh mục dải phụ tải
4.	Danh mục ngày ghi
III	Quản lý chức năng khai báo cấu hình
1.	Cập nhật thiết kế dải phụ tải của đơn vị
2.	Cập nhật thiết kế nhóm phụ tải của đơn vị

STT	Danh sách chức năng
3.	Cập nhật thiết kế thành phần phụ tải của đơn vị
IV	Quản lý chức năng nhận số liệu
1.	Nhận số liệu kết quả nghiên cứu phụ tải của đơn vị
2.	Kiểm tra số liệu theo từng dải nghiên cứu
V	Quản lý chức năng xem báo cáo
1.	PL1-1: Biểu đồ phụ tải điện của phân nhóm phụ tải điện
2.	PL1-2: Biểu đồ phụ tải điện của nhóm phụ tải điện
3.	PL1-3: Biểu đồ phụ tải điện của thành phần phụ tải điện
4.	PL1-4: Biểu đồ phụ tải của hệ thống điện miền
5.	PL1-5.1 Biểu đồ phụ tải điện theo đơn vị - Biểu đồ phụ tải điện ngày điển hình
6.	PL1-5.2 Biểu đồ phụ tải điện theo đơn vị - Biểu đồ thống kê công suất LDC
7.	PL1-5.3 Biểu đồ phụ tải điện theo đơn vị - Đồ thị tỷ lệ phần trăm của công suất phụ tải điện
8.	PL2-A-1: Phân tích biểu đồ của phân nhóm phụ tải điện
9.	PL2-A-2: Phân tích biểu đồ của nhóm phụ tải điện
10.	PL2-A-3: Phân tích biểu đồ của thành phần phụ tải điện
11.	PL2-A-4: Phân tích biểu đồ phụ tải điện của các Đơn vị phân phối điện
12.	PL2-A-5: Phân tích biểu đồ phụ tải điện của các Đơn vị trong Tập đoàn
13.	PL2-A-6: Phân tích biểu đồ phụ tải điện của hệ thống điện quốc gia
14.	PL2-B-1: Phân tích xu hướng thay đổi trong biểu đồ phụ tải điện của phân nhóm phụ tải điện
15.	PL2-B-2: Phân tích xu hướng thay đổi trong biểu đồ phụ tải điện của nhóm phụ tải điện
16.	PL2-B-3: Phân tích xu hướng thay đổi trong biểu đồ phụ tải điện của nhóm phụ tải điện
17.	PL2-B-4: Phân tích xu hướng thay đổi trong biểu đồ phụ tải điện của thành phần phụ tải điện

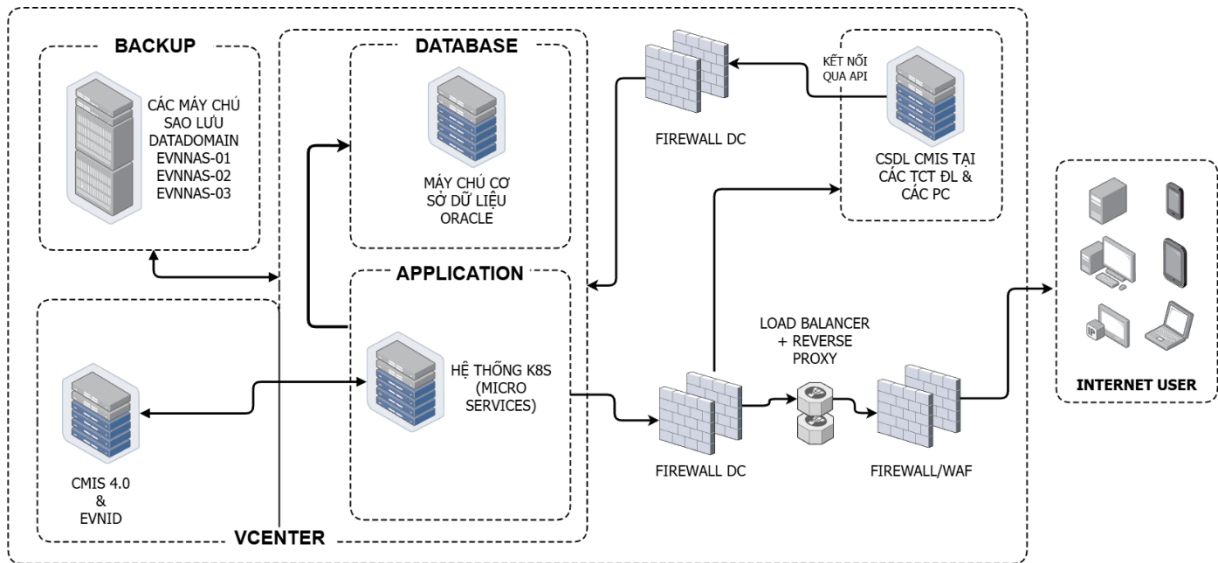
STT	Danh sách chức năng
18.	PL2-B-5 Phân tích xu hướng thay đổi trong biểu đồ phụ tải điện của Đơn vị phân phối điện
19.	PL2-C-1: Phân tích tăng trưởng (%) điện năng và công suất của phân nhóm phụ tải điện
20.	PL2-C-2: Phân tích tăng trưởng (%) điện năng và công suất của nhóm phụ tải điện
21.	PL2-C-3: Phân tích tăng trưởng (%) điện năng và công suất của thành phần phụ tải điện
22.	PL2-C-4: Phân tích tăng trưởng (%) điện năng và công suất của Đơn vị phân phối điện

2.1.4. Thiết kế cơ sở dữ liệu

STT	Danh sách bảng
I	QUẢN LÝ DANH MỤC
1	Danh mục thành phần phụ tải
2	Danh mục cấu hình
3	Danh mục đơn vị quản lý
4	Danh mục dải phụ tải
5	Danh mục ngày ghi
II	QUẢN TRỊ HỆ THỐNG
1	Chức năng hệ thống
2	Lịch sử đăng nhập/đăng xuất
3	Phân quyền role cho tổ chức
4	Phân quyền user cho tổ chức
5	Phân quyền chức năng theo role
6	Phân quyền chức năng theo user
7	Quản lý refresh token
8	Role
9	User
10	Thiết bị user
11	Nhật ký user
12	Quan hệ phân quyền role-user
13	Tham số hệ thống
III	ĐỒNG BỘ DỮ LIỆU
1	Dữ liệu kết quả nghiên cứu phụ tải của đơn vị
2	Dữ liệu đồng bộ với CMIS
3	Dữ liệu báo cáo và biểu đồ

2.2. Phương án hạ tầng kỹ thuật phục vụ phát triển, triển khai

2.2.1. Mô hình hạ tầng



Mô hình hệ thống tổng thể

Vùng máy chủ nội bộ: Gồm 02 zone chính, zone database đặt máy chủ cơ sở dữ liệu Oracle, cung cấp dịch vụ cơ sở dữ liệu cho hệ thống Nghiên cứu phụ tải (NCPT). Zone Application đặt cụm máy chủ Kubernetes (K8s) cung cấp các API và dịch vụ Microservices cho hệ thống.

Vùng mạng WAN: phân hệ phục vụ kết nối WAN tới hạ tầng mạng của các đơn vị trong EVN,. Trong phân vùng này sẽ có các thiết bị định tuyến và chuyển mạch kết nối giữa các đơn vị cũng như người dùng nội bộ.

Vùng Internet User: người dùng kết nối tới hệ thống nằm ngoài hệ thống WAN, LAN nội bộ của EVN. Người dùng sẽ kết nối tới hệ thống NCPT thông qua kết nối internet tới địa chỉ Domain *.evn.com.vn được public.

Vùng máy chủ Backup (Sao lưu): quy hoạch riêng cho các máy chủ vật lý cung cấp dịch vụ sao lưu dữ liệu chuyên dụng tại EVN.

Cụm máy chủ Vcenter: Gồm toàn bộ các máy chủ phiên tại EVN, cung cấp dịch vụ ảo hóa cho toàn bộ hệ thống CNTT.

2.2.2. Danh mục các thiết bị/phần mềm yêu cầu:

- Danh mục các thiết bị/máy chủ phục vụ hệ thống

Căn cứ vào mức độ sử dụng thực tế của dịch vụ hệ thống đã nêu trong phần hiện trạng (CSDL, Ứng dụng, sao lưu dữ liệu ..) Hệ thống NCPT nâng cấp cần đáp ứng được các nhu cầu dữ liệu hiện tại và sự tăng trưởng trong tương lai, dự kiến đề xuất như sau:

STT	Tên thiết bị/ phần mềm	Số lượng	Mô tả/ Mục đích sử dụng	Thông số kỹ thuật và các tiêu chuẩn (tối thiểu)
1	Máy chủ Cơ sở dữ liệu NCPT-DB-XX (Hostname sẽ được đặt tên cụ thể sau khi tạo dựng)	01	Đóng vai trò lưu trữ cơ sở dữ liệu hệ thống NCPT,	- CPU: ≥ 16 core, tốc độ tương đương 2.4GHz - RAM: ≥ 32 GB - Ổ cứng: \geq OS: 150 GB; DATA: 300 GB
2	Hệ thống K8s	-	Cung cấp các micro-service cho dịch vụ của hệ thống	

• Danh mục các thiết bị phục vụ kết nối hệ thống

STT	Tên thiết bị	Mô tả	Diễn giải	Ghi chú
1	FW- INTERNAL -01	Cặp thiết bị firewall Palo Alto 3440 -PAN-OS phiên bản 11.2.4-h1 -License Partner Support, Threat Prevention	Tường lửa dùng chung trên hệ thống, thực hiện định tuyến, phân chia và kiểm soát giao dịch giữa các vùng mạng Vùng mạng cho máy chủ các đối tác.	DC 11 Cửa Bắc
2	FW-INTERNAL-02			
3	TOR SW 109 APP-01	Thiết bị switch Juniper EX4300	Switch dùng chung, cung cấp các kết nối mạng cho các máy chủ, thiết bị tại vùng mạng Database, Application và Backup	DC 11 Cửa Bắc
4	TOR SW 109 APP-02			
5	TOR SW 210 BACKUP-01			
6	TOR SW 210 BACKUP-02			
7	TOR SW 108 DATABASE-01			
8	TOR SW 108 DATABASE-02			

• Yêu cầu phần mềm cài đặt

Server	Phần mềm cài đặt
Ứng dụng	Nginx
Cơ sở dữ liệu	Oracle Database 19C

- Phương án cho các thiết bị/máy chủ/phần mềm phục vụ hệ thống

Tổng thể hệ thống Nghiên cứu phụ tải (NCPT) sẽ được triển khai gồm 01 máy chủ cơ sở dữ liệu được cấp phát trên hạ tầng máy chủ ảo hóa Vcenter 90, Vcenter 70 hoặc Vcenter 45, dịch vụ ứng dụng sẽ được triển khai trên hệ thống K8s, khai thác tài nguyên trên các máy chủ phiên và hệ thống lưu trữ SAN hiện hữu tại EVNICT. Cụ thể như sau:

- Máy chủ cơ sở dữ liệu (CSDL) được cấp tại phân vùng Database. Để nâng cao tính an toàn và liên tục của dịch vụ, giảm thời gian Downtime khi xảy ra sự cố và thời gian khôi phục dịch vụ.

- Đối với ứng dụng của hệ thống được cấp phát qua các Micro service trên hệ thống K8s tại EVNICT. Dịch vụ Website của hệ thống sẽ được truy cập từ trong WAN hoặc từ ngoài Internet qua hệ thống Firewall cũng như Load Balancer ...

- Cơ sở dữ liệu Oracle phiên bản 19C hiện triển khai không yêu cầu mua license, đối với phần mềm Nginx là phần mềm mã nguồn mở và miễn phí.

- Phương án cho các thiết bị phục vụ kết nối hệ thống

- Dữ liệu của hệ thống sẽ được tiếp nhận và trao đổi qua các hệ thống thành phần như:

- + Hệ thống EVNID

- + Hệ thống CMIS tại các Tổng công ty Điện lực

- Quy hoạch các vùng mạng và địa chỉ IP trong hệ thống mạng tại DC của EVN:

- + Vùng mạng biên: không áp dụng do là hệ thống đóng. Hệ thống sử dụng vùng Secure Server như vùng mạng biên để kết nối đi các vùng khác.

- + Vùng DMZ: cung cấp dịch vụ ra Internet.

- + Hệ thống NCPT không có kết nối mạng không dây nên không thiết lập vùng mạng không dây.

- + Vùng mạng nội bộ chia thành nhiều vùng nhỏ hơn để đáp ứng nhu cầu kiểm soát giao dịch giữa các dịch vụ có yêu cầu về mức độ an toàn khác nhau:

- Vùng mạng cho máy chủ ứng dụng (Application);

- Vùng mạng cho máy chủ cơ sở dữ liệu (Database).

- ồng mạng Sao lưu dữ liệu (Backup)
- Quy hoạch địa chỉ IP của hệ thống
 - + Vùng máy chủ CSDL của hệ thống: thuộc vùng Database trong hệ thống mạng của EVN.
 - + Vùng máy chủ ứng dụng của hệ thống: thuộc vùng Application trong hệ thống mạng của EVN.
 - + Vùng máy chủ sao lưu dữ liệu của hệ thống: thuộc vùng mạng Application trong hệ thống mạng của EVN.

2.3. Cấp độ an toàn thông tin

Đáp ứng yêu cầu cấp độ 2 về đảm bảo an toàn hệ thống thông tin quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ.

Mục 3. Yêu cầu kỹ thuật của gói thầu:

3.1. Phạm vi cung cấp dịch vụ

- Khảo sát thu thập thông tin và xây dựng Phương án triển khai kiểm tra, đánh giá ANM&ATTT
- Kiểm tra, đánh giá ANM&ATTT hệ thống gồm:
 - Đánh giá điểm yếu cho mã nguồn ứng dụng
 - Đánh giá điểm yếu cho thư viện
 - Đánh giá điểm yếu và kiểm thử xâm nhập cho API
 - Đánh giá điểm yếu và kiểm thử xâm nhập cho ứng dụng
 - Đánh giá điểm yếu và kiểm thử xâm nhập cho hạ tầng CNTT
 - Tổng hợp và lập báo cáo đánh giá ANM&ATTT
- Tái đánh giá ANM&ATTT và báo cáo tái đánh giá kết quả khắc phục lỗ hổng

3.2. Yêu cầu giải pháp kỹ thuật và biện pháp tổ chức cung cấp dịch vụ

3.2.1. Hình thức thực hiện

Đánh giá trực tiếp tại chỗ theo hình thức whitebox. Đơn vị thực hiện kiểm tra, đánh giá điểm yếu và kiểm thử xâm nhập được cung cấp đầy đủ thông tin cũng như đặc quyền đối với hệ thống.

3.2.2. Khảo sát thu thập thông tin và xây dựng Phương án triển khai kiểm tra, đánh giá ANM&ATTT

- Khảo sát thiết kế
- Khảo sát ứng dụng

- Khảo sát hạ tầng CNTT
- Lập kế hoạch kiểm tra và đánh giá Phương án triển khai kiểm tra, đánh giá ANM&ATTT trình chủ đầu tư phê duyệt trước khi triển khai, bao gồm nhưng không giới hạn các nội dung sau:
 - Phương án, đề xuất kế hoạch thực hiện;
 - Công cụ sử dụng;
 - Kế hoạch thực hiện.

3.2.3. Kiểm tra, đánh giá ANM&ATTT hệ thống

a) Đánh giá điểm yếu mã nguồn ứng dụng

- Dựa trên các mô tả lỗ hổng trong danh sách OWASP Code Review Guide 2.0 do tổ chức OWASP đưa ra:

STT	Mô tả
1	A1 - Injection
2	A2 - Broken Authentication and Session Management
3	A3 - Cross-site Scripting (XSS)
4	A4 - Insecure Direct Object Reference
5	A5 - Security Misconfiguration
6	A6 - Sensitive Data Exposure
7	A7 - Missing Function Level Access Control
8	A8 - Cross-site Request Forgery (CSRF)
9	A9 - Using Components with Known Vulnerabilities
10	A10 - Unvalidated Redirects and Forwards

- Dựa trên Quyết định số 1290/QĐ-EVN ngày 05/09/2022 của Tập đoàn Điện lực Việt Nam:

Nội dung quy tắc	Yêu cầu	Mục đích	Tài liệu tham chiếu
Thông tin định danh	Tên đăng nhập phải là duy nhất, không phân biệt hoa thường, chỉ nên chứa tập các ký tự là chữ cái, chữ số, dấu gạch dưới.	Bảo vệ tài khoản người dùng.	OWASP Secure Coding Practices: Mục

Nội dung quy tắc	Yêu cầu	Mục đích	Tài liệu tham chiếu
	<p>Thiết lập chính sách mật khẩu mạnh theo yêu cầu tại quy định chính sách mật khẩu mạnh hiện hành của EVN ban hành.</p> <p>Thiết lập thời gian hết hiệu lực cho mật khẩu tối đa 90 ngày, mật khẩu mới không được trùng với mật khẩu hiện tại.</p> <p>Đối với chức năng reset/quên mật khẩu:</p> <p>Đường dẫn reset/quên mật khẩu được gửi qua email phải bị mất hiệu lực sau lần truy cập đầu tiên hoặc sau 8 giờ nếu không được truy cập.</p> <p>Nếu chức năng reset/quên mật khẩu thực hiện gửi mật khẩu qua email, tin nhắn thì mật khẩu phải được sinh ngẫu nhiên và phải tuân theo chính sách mật khẩu mạnh.</p> <p>Nếu chức năng reset/quên mật khẩu sử dụng mã OTP để kiểm tra xác nhận từ người dùng, việc sử dụng mã OTP (hướng dẫn tại mục 9 trong cùng tài liệu này).</p> <p>Chỉ lưu dạng mã hash của mật khẩu, mã PIN trong database (DB), sử dụng thuật toán hash từ SHA-256, SHA-512, SHA-3 và các thuật toán tương đương.</p>		<p>“Authentication and Password Management”</p>
<p>Quản lý phiên đăng nhập</p>	<p>Session phải được quản lý bởi server, sinh ngẫu nhiên và độ dài tối thiểu là 128-bit.</p> <p>Session phải được thiết lập thời gian timeout, giá trị timeout nên cân bằng giữa nhu cầu thương mại và yếu tố bảo mật.</p> <p>Tạo mới session sau khi đăng nhập thành công.</p> <p>Xóa giá trị session id và các dữ liệu gắn với session đó khi người dùng đăng xuất.</p> <p>Cấu hình thuộc tính “Secure” đối với các ứng dụng sử dụng HTTPS và “HTTP-Only” cho trường Cookie.</p> <p>Đối với các chức năng quan trọng có tương tác với database, ứng với mỗi</p>	<p>Bảo vệ phiên đăng nhập của người dùng</p>	<p>OWASP Secure Coding Practices: Mục “Session Management”</p>

Nội dung quy tắc	Yêu cầu	Mục đích	Tài liệu tham chiếu
	phiên phải sinh thêm 1 token ngẫu nhiên, và thực hiện kiểm tra tính hợp lệ của token này trước khi xử lý truy vấn từ người dùng.		
Phân quyền	<p>Kiểm tra phân quyền dựa trên các đối tượng được lưu tại server (ví dụ: tham số lưu trên session server, dữ liệu lưu trên DB,...).</p> <p>Phân quyền tối thiểu, chỉ đáp ứng đủ chức năng và tài nguyên cho người dùng/ứng dụng.</p> <p>Phía giao diện người dùng: Chỉ hiển thị các thành phần giao diện, đường dẫn, hàm,... tương ứng với quyền của người dùng.</p> <p>Phía server: Kiểm tra quyền tác động của người dùng/ứng dụng trên các hàm và tài nguyên tương ứng trước khi thực hiện bất cứ tác vụ nào tới hệ thống.</p> <p>Nên có tính năng xóa phiên làm việc hiện tại của người dùng hoặc các cơ chế tương đương đối với các trường hợp quyền người dùng bị thay đổi hoặc bị disable bởi người dùng có thẩm quyền.</p> <p>Không đặt trang quản trị public internet, trong trường hợp bắt buộc phải đặt public phải giới hạn các IP được phép truy cập hoặc sử dụng cơ chế xác thực đa nhân tố.</p>	Bảo vệ dữ liệu của ứng dụng	OWASP Secure Coding Practices: Mục "Access Control"
Mã hóa các dữ liệu nhạy cảm	Đối với các loại dữ liệu nhạy cảm như thông tin tài khoản ngân hàng, private key... phải thực hiện mã hóa trước khi lưu trữ, sử dụng thuật toán AES-256 hoặc các thuật toán tương đương.	Bảo vệ các dữ liệu nhạy cảm	OWASP Secure Coding Practices: Mục "Cryptographic Practices"
Tương tác với back-end - SQL	Sử dụng mô hình truy vấn prepared statement (parameterized query) hoặc các hình thức tương đương.	Đảm bảo việc truy cập dữ liệu bằng SQL	OWASP Secure Coding Practices:

Nội dung quy tắc	Yêu cầu	Mục đích	Tài liệu tham chiếu
	Trong 1 số trường hợp không sử dụng được các mô hình ở trên, phải thiết lập danh sách whitelist các đầu vào mong muốn.	an toàn	Mục “Database Security”
Tương tác với back-end - NoSQL	Không công khai dịch vụ ra mạng internet, cài đặt trong môi trường mạng an toàn. Đối với các hệ NoSQL có hỗ trợ xác thực, phải cấu hình xác thực khi truy cập. Phụ thuộc vào hệ NoSQL sử dụng, sử dụng các api hỗ trợ truy vấn an toàn hoặc thực hiện escape các ký tự đặc biệt khi xây dựng câu truy vấn.	Đảm bảo việc truy cập dữ liệu bằng NoSQL an toàn	
Tương tác với back-end - XPath	Thiết lập danh sách whitelist các ký tự đầu vào mong muốn, đầu vào nên là tập hợp của chữ cái, chữ số. Lập danh sách blacklist các ký tự đặc biệt (() = ‘ [] : , * / và dấu cách), loại bỏ các đầu vào có chứa các ký tự nằm trong blacklist.	Đảm bảo việc truy cập dữ liệu bằng XPath an toàn	
Tương tác với back-end - LDAP	Thiết lập danh sách whitelist các ký tự đầu vào mong muốn, đầu vào nên là tập hợp của chữ cái, chữ số. Lập danh sách blacklist các ký tự đặc biệt (() ; , * & = và nullbyte), loại bỏ các đầu vào có chứa các ký tự nằm trong blacklist.	Đảm bảo việc truy cập dữ liệu bằng LDAP an toàn	
Tương tác với back-end - Tương tác với OS	Sử dụng các API hỗ trợ việc thực thi câu lệnh hệ thống. Không truyền trực tiếp dữ liệu người dùng truyền lên tới OS, trong trường hợp bắt buộc phải thiết lập danh sách whitelist các đầu vào mong muốn.	Đảm bảo việc tương tác với OS	
Tương tác với back-end - Tương tác	Không truyền trực tiếp dữ liệu từ người dùng đến các hàm include file. Lập danh sách whitelist các định dạng file được phép upload tùy theo nghiệp vụ hệ	Đảm bảo việc tương tác với file	

Nội dung quy tắc	Yêu cầu	Mục đích	Tài liệu tham chiếu
với file	<p>thông (khuyến nghị các loại file như docx, xlsx, pdf, png, jpg). Validate file hợp lệ này bằng cách kiểm tra phần mở rộng của file tương ứng với whitelist định dạng file được upload.</p> <p>Với các trường hợp không bắt buộc thì không lưu file upload trong thư mục web, bỏ quyền thực thi trên thư mục upload.</p> <p>Khi cần ánh xạ tới các file tồn tại trên hệ thống phải thiết lập danh sách whitelist đầu vào mong muốn hoặc gán các giá trị định danh tương ứng file thay vì truyền tên file.</p> <p>Không trả về đường dẫn tuyệt đối của file.</p> <p>Tất cả dữ liệu, tài nguyên hệ thống (báo cáo, file upload, file cấu hình...) không được lưu trong thư mục cho phép truy cập trực tiếp không qua xác thực.</p>		
Tương tác với back-end - Xử lý back-end HTTP request	<p>Khi tạo HTTP request phía server, các tham số GET, POST cho request đó tránh tạo từ dữ liệu phía người dùng, hoặc phải được kiểm tra cẩn thận để chống ghi đè các tham số khác.</p> <p>Không lấy địa chỉ server từ dữ liệu người dùng gửi lên. Trong trường hợp địa chỉ server cần lấy từ người dùng, phải blacklist các IP trong dải nội bộ sau khi đã phân giải DNS.</p>	Đảm bảo việc Xử lý back-end HTTP request an toàn	
Tương tác với back-end - XML	<p>Tắt tính năng “external entity resolve” và “remote doctype retrieval” của xml parser khi đọc dữ liệu xml.</p> <p>Kiểm tra dữ liệu người dùng, encode các kí tự đặc biệt (<>'") khi tạo dữ liệu xml.</p>	Đảm bảo việc truy cập dữ liệu bằng XML an toàn	
Tương tác với back-end - deserialize	<p>Khuyến nghị chỉ thực hiện deserialize các dữ liệu từ các nguồn tin cậy, an toàn hoặc sử dụng kiểu dữ liệu json.</p> <p>Các trường hợp nằm ngoài mục 4.10.1</p>	Đảm bảo việc thực hiện deserialize an toàn	

Nội dung quy tắc	Yêu cầu	Mục đích	Tài liệu tham chiếu
	<p>phải thực hiện thêm 1 trong 2 tác vụ sau:</p> <p>Sinh 1 mã bí mật (S) và lưu tại server. Khi cần gửi dữ liệu đã được serialize (D), gửi kèm mã hash được tính theo công thức: $H = \text{hash}(D+S)$.</p> <p>Khi cần deserialize dữ liệu D, thực hiện sinh mã $H1 = \text{hash}(D+S)$, nếu H và H1 trùng khớp mới thực hiện deserialize D.</p> <p>Thiết lập whitelist các class được deserialize. Kiểm tra tên các class trong phần dữ liệu, nếu các class này thuộc whitelist mới thực hiện deserialize dữ liệu.</p>		
Kiểm soát dữ liệu đầu vào	<p>Việc kiểm tra dữ liệu đầu vào phải được thực hiện phía server.</p> <p>Thực hiện việc kiểm tra dữ liệu từ tất cả các nguồn dữ liệu có tương tác với người dùng (Các tham số lấy từ GET/POST request, HTTP Headers, dữ liệu lấy từ DB, dữ liệu từ file upload,...).</p> <p>Xác định 1 kiểu encoding nhất quán sử dụng khi hiển thị, trao đổi hay lưu trữ dữ liệu. Chỉ thực hiện filter, validate dữ liệu sau khi đã đưa dữ liệu về kiểu encoding đã xác định trước đó.</p> <p>Validate kiểu dữ liệu, phạm vi, kích thước dữ liệu và định dạng dữ liệu.</p> <p>Nếu dữ liệu đầu vào bắt buộc là các ký tự đặc biệt, phải thiết lập danh sách whitelist các ký tự đầu vào mong muốn.</p>	Đảm bảo dữ liệu đầu vào an toàn	OWASP Secure Coding Practices: Mục "Input Validation"
Kiểm soát dữ liệu đầu ra	<p>Phải chỉ rõ character encoding cho dữ liệu đầu ra.</p> <p>Phải thiết lập giá trị Content-type tương ứng với định dạng dữ liệu trả về (ví dụ dữ liệu json phải tương ứng với Content-type là application/json)</p> <p>Response body phải được encode theo ngữ cảnh sử dụng. Ví dụ: Đầu ra là html, thực hiện html encode các ký tự đặc biệt</p>	Đảm bảo dữ liệu đầu ra an toàn	OWASP Secure Coding Practices: Mục "Output Encoding"

Nội dung quy tắc	Yêu cầu	Mục đích	Tài liệu tham chiếu
	<p>(<>'"&) từ các nguồn dữ liệu không an toàn (Các tham số lấy từ GET/POST request, HTTP Headers, dữ liệu lấy từ DB, dữ liệu từ file upload,... có thể điều khiển được bởi người dùng).</p> <p>Response header: lọc bỏ các kí tự đặc biệt (\n, \r) do dữ liệu người dùng truyền vào.</p> <p>Cookie trả về phải giới hạn tối thiểu nhất các thuộc tính (domain, path, httponly, expire, secure). Tránh lưu trữ các dữ liệu nhạy cảm trên cookie, nếu cần lưu trữ các dữ liệu nhạy cảm thì phải thực hiện mã hóa các dữ liệu này với thuật toán đối xứng mạnh và key chỉ được lưu trên server.</p> <p>Hạn chế việc chuyển hướng, chuyển tiếp đến các URI khác. Nếu ứng dụng có chức năng này phải lập danh sách whitelist các địa chỉ server được phép thực hiện chuyển hướng, chuyển tiếp.</p>		
Kiểm soát ngoại lệ và ghi log ứng dụng	<p>Xử lý các ngoại lệ bằng try-catch và trả về các thông báo lỗi chung, thông báo lỗi trả về không được chứa các thông tin nhạy cảm của người dùng, hệ thống,...</p> <p>Các thông tin lỗi, ngoại lệ này phải được log lại để phục vụ bảo trì, xác định nguyên nhân lỗi ứng dụng.</p> <p>File log phải được đặt tại thư mục an toàn ngoài thư mục web.</p> <p>Không log lại các dữ liệu nhạy cảm (thông tin người dùng, session id, thông tin hệ thống).</p> <p>Giới hạn người dùng cho phép truy cập file log.</p>	Đảm bảo ghi log an toàn	OWASP Secure Coding Practices: Mục "Error Handling and Logging"
Sử dụng framework, thư viện (third-party component)	<p>Loại các code thừa, các thành phần và thư viện không cần thiết.</p> <p>Sử dụng phiên bản mới nhất của framework, thư viện tại thời điểm phát triển ứng dụng.</p>	Đảm bảo sử dụng framework an toàn	OWASP Secure Coding Practices: Mục "System"

Nội dung quy tắc	Yêu cầu	Mục đích	Tài liệu tham chiếu
	<p>Thường xuyên cập nhật các bản vá lỗi cho framework, thư viện.</p> <p>Tắt chế độ development của framework khi triển khai ứng dụng thực tế.</p>		Configurati on”
Xử lý business logic	<p>Lập trình viên phải nắm rõ được toàn bộ luồng nghiệp vụ của ứng dụng, phải xác định các ngoại lệ cho từng nghiệp vụ để tránh các lỗi logic có thể xảy ra.</p> <p>Các chức năng quan trọng (ví dụ chuyển khoản ngân hàng), sử dụng các hình thức khóa hoặc các hình thức tương đương để tránh lỗi race condition.</p> <p>Đối với các dịch vụ viễn thông, khi khách hàng đăng ký các dịch vụ các dịch vụ gia tăng trên điện thoại di động (VAS) phải có tin nhắn thông báo tới khách hàng.</p> <p>Đối với các giao dịch chuyển tiền, ví dụ chuyển từ tài khoản A sang tài khoản B: phải thực hiện trừ tiền tài khoản A thành công rồi mới được thực hiện cộng tiền vào tài khoản B.</p> <p>Đối với các ứng dụng có chức năng gửi tin nhắn tới người dùng phải giới hạn số lần gửi tin trong 1 ngày ứng với mỗi đầu số nhận tin. Đối với chức năng quan trọng như đăng ký, lấy lại mật khẩu chỉ cho phép gửi ≤ 3 tin/ngày.</p> <p>Yêu cầu khi sử dụng và sinh mã OTP:</p> <p>Giới hạn số lần nhập sai với mỗi mã OTP ≤ 3 lần/ngày, xóa mã cũ và sinh mã mới khi nhập sai vượt quá số lần cho phép.</p> <p>Không được sử dụng mã OTP làm mật khẩu.</p>	Đảm bảo xử lý logic an toàn	

b) Đánh giá điểm yếu thư viện

- Sử dụng thông tin thu thập được để rà soát, kiểm tra các thư viện (open-source, third-party)
- Tìm kiếm, phân tích các lỗ hổng bảo mật đã biết của thư viện (CVE), rủi ro từ dependency, phiên bản lỗi thời

- Dựa trên quy tắc sử dụng framework, thư viện (third-party component) trong Quyết định số 1290/QĐ-EVN ngày 05/09/2022 của Tập đoàn Điện lực Việt Nam:

- Loại các code thừa, các thành phần và thư viện không cần thiết.
- Sử dụng phiên bản mới nhất của framework, thư viện tại thời điểm phát triển ứng dụng.
- Thường xuyên cập nhật các bản vá lỗi cho framework, thư viện.
- Tắt chế độ development của framework khi triển khai ứng dụng thực tế.

c) Đánh giá điểm yếu và kiểm thử xâm nhập API

- Dựa trên các mô tả lỗ hổng trong danh sách OWASP Top 10 API Security Risks năm 2023 do tổ chức OWASP đưa ra:

STT	Mô tả
1	API1:2023 - Broken Object Level Authorization
2	API2:2023 - Broken Authentication
3	API3:2023 - Broken Object Property Level Authorization
4	API4:2023 - Unrestricted Resource Consumption
5	API5:2023 - Broken Function Level Authorization
6	API6:2023 - Unrestricted Access to Sensitive Business Flows
7	API7:2023 - Server-Side Request Forgery
8	API8:2023 - Security Misconfiguration
9	API9:2023 - Improper Inventory Management
10	API10:2023 - Unsafe Consumption of APIs

- Dựa trên hướng dẫn tại văn bản số 555/EVN-VTCNTT ngày 09/02/2023 của Tập đoàn Điện lực Việt Nam:

STT	Yêu cầu đảm bảo ATTT cho các API
1	<p><i>Authentication - Các API phải được xác thực khi truy cập</i></p> <p><i>a. Mục đích:</i> ngăn chặn truy nhập ứng dụng một cách trái phép</p> <p><i>b. Các yêu cầu và khuyến nghị:</i></p> <ul style="list-style-type: none"> - Việc truy xuất các API cần được bảo vệ bằng JWT. Tạo JWT áp dụng phương pháp cặp private key và public key;

STT	Yêu cầu đảm bảo ATTT cho các API
	<ul style="list-style-type: none"> - Bổ sung các xác thực khác như xác thực app truy cập để kiểm soát request truy cập; - Server kiểm tra tính hợp lệ của token trước khi cung cấp tài nguyên cho client; - Token có thời gian sống/tồn tại ngắn (tối đa 1 ngày tùy từng giao dịch), không để thời gian sống/tồn tại vĩnh viễn; - Mật khẩu người dùng yêu cầu bắt buộc đặt phức tạp (gồm chữ, số và ký tự đặc biệt) và phải có cơ chế mã hóa tốt; - Thông tin lưu trong JWT cần tối thiểu và phải kiểm tra thông tin đó phía server trước khi truy xuất tài nguyên; - Các API phải sử dụng TLS – Transport Layer Security (https thay vì http).
2	<p><i>Authorization - Các API phải được kiểm tra quyền truy cập</i></p> <p><i>a. Mục đích:</i> ngăn chặn truy cập ứng dụng trái phép, giảm thiểu rủi ro bị tấn công dạng IDOR (Insecure Direct Object Reference) – Tham chiếu các đối tượng không bảo mật.</p> <p><i>b. Các yêu cầu và khuyến nghị:</i></p> <ul style="list-style-type: none"> - Kiểm tra quyền truy cập của API trước khi thực thi và trả về dữ liệu: yêu cầu xem xét quyền truy cập theo chức năng và dữ liệu được truy cập; - Phân tách các API cho các mục đích khác nhau như API quản trị, API nội bộ, API public (đối với các API public, thông tin cung cấp chỉ bao gồm các thông tin cơ bản, hạn chế tối thiểu về các thông tin định danh cá nhân, API nội bộ cho các chức năng đối với CBCNV sử dụng cùng hệ thống); - Đối với việc truy xuất tài nguyên thông qua các khóa chính khuyến cáo khóa chính phải để dạng tự sinh ngẫu nhiên, không sử dụng phương pháp tự tăng tuần tự.
3	<p><i>Excessive Data Exposure</i></p> <p><i>a. Mục đích:</i> kiểm soát dữ liệu server trả về cho client trong mỗi giao dịch</p> <p><i>b. Các yêu cầu và khuyến nghị:</i></p> <ul style="list-style-type: none"> - Các API không được quyền trả về dữ liệu quá dư thừa so với yêu cầu của client (thường phục vụ cho việc filter dữ liệu tại client); - Xác định rõ thông tin cần trả về từ server tránh trả về các thông tin nhạy cảm, không cần thiết.
4	<p><i>Mass Assignment - Kiểm tra các dữ liệu cập nhật</i></p> <p><i>a. Mục đích:</i> kiểm soát các trường thông tin cập nhật và hệ thống</p> <p><i>b. Các yêu cầu và khuyến nghị:</i></p> <ul style="list-style-type: none"> - Việc cập nhật dữ liệu: chỉ hiển thị và cập nhật các trường dữ liệu; - Tạo các module trung gian và kiểm tra dữ liệu trước khi gán vào

STT	Yêu cầu đảm bảo ATTT cho các API
	object trong hệ thống.
5	<p><i>Security Misconfiguration - Các lưu ý về cấu hình API</i></p> <p>a. Mục đích: kiểm soát cấu hình các hệ thống developer, test và product</p> <p>b. Các yêu cầu và khuyến nghị:</p> <ul style="list-style-type: none"> - Tắt chế độ debug; - Không sử dụng các thông tin mặc định; - Bổ sung CORS (Cross – Origin – Resource – Sharing) policy; - Kiểm soát các hàm không cần thiết khi tạo CRUD API; - Kiểm soát các thông báo API trả ra đặc biệt khi có lỗi.
6	<p><i>Injection</i></p> <p>a. Mục đích: kiểm soát các ngoại lệ xảy ra trong hệ thống</p> <p>b. Các yêu cầu và khuyến nghị:</p> <ul style="list-style-type: none"> - Kiểm tra, kiểm soát các lỗi injection (SQL, noSQL, OS Command...); - Kiểm soát dữ liệu đầu vào, các trường giá trị (field value) phải được validate, ngay cả dữ liệu output cũng phải được kiểm tra để hạn chế tối đa việc lộ thông tin nhạy cảm.
7	<p><i>Improper Assets Management - Kiểm soát tài nguyên</i></p> <p>a. Mục đích: kiểm soát các tài nguyên cung cấp của hệ thống, loại bỏ hoặc hạn chế các API dư thừa, không sử dụng</p> <p>b. Các yêu cầu và khuyến nghị:</p> <ul style="list-style-type: none"> - Hạn chế truy cập vào những API chưa được công khai (các API dùng để kiểm tra, hỗ trợ, chưa được sử dụng...), đồng thời bổ sung các quyền đặc biệt nếu cần truy cập; - Trong môi trường thử nghiệm, fix, bug cần hạn chế truy cập vào dữ liệu trên hệ thống thực tế (product). Thực hiện đồng bộ giữa môi trường thử nghiệm và phát triển, nhằm kiểm soát chặt chẽ các API chưa được fix lỗi có thể truy cập vào dữ liệu thực tế; - Triển khai sử dụng firewall hoặc một số biện pháp kiểm soát bên ngoài truy cập các API. - Lưu trữ và Up – To – Date các tài liệu liên quan, các mô tả API.
8	<p><i>Insufficient Logging & Monitoring - Ghi log và giám sát</i></p> <p>a. Mục đích: theo dõi kiểm tra hoạt động của ứng dụng thông các log</p> <p>b. Các yêu cầu và khuyến nghị:</p> <ul style="list-style-type: none"> - Ghi lại chi tiết tất cả những failure trong hệ thống, đặc biệt là các failure về AuthN và AuthZ, các Security check như CORS policy, field value validation; - Log được cung cấp theo đúng định dạng mà các tool giám sát có thể xử lý tự động được. Đúng định dạng nhưng phải đúng và đầy đủ dữ liệu để có bất cứ issue nào phát sinh, cũng có thể nhanh chóng tìm được nguyên nhân;

STT	Yêu cầu đảm bảo ATTT cho các API
	<ul style="list-style-type: none"> - Phải bảo vệ log vì đây là các thông tin quan trọng, tránh các đối tượng không liên quan có thể khai thác log hệ thống; - Không được lưu trữ thông tin nhạy cảm trong log.

d) Đánh giá điểm yếu và kiểm thử xâm nhập ứng dụng Web

- Dựa trên các mô tả lỗ hổng trong danh sách OWASP Top 10 năm 2021 do tổ chức OWASP đưa ra:

STT	Mô tả
1	A01:2021 - Broken Access Control
2	A02:2021 - Cryptographic Failures
3	A03:2021 - Injection
4	A04:2021 - Insecure Design
5	A05:2021 - Security Misconfiguration
6	A06:2021 - Vulnerable and Outdated Components
7	A07:2021 - Identification and Authentication Failures
8	A08:2021 - Software and Data Integrity Failures
9	A09:2021 - Security Logging and Monitoring Failures
10	A10:2021 - Server-Side Request Forgery (SSRF)

- Dựa trên Quyết định số 742/QĐ-BTTTT ngày 22/04/2022 quy định Yêu cầu an toàn cơ bản đối với Phần mềm nội bộ cấp độ 2:

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin
			2
1	Xác thực		
1.1	Có chức năng xác thực người sử dụng khi truy cập, quản trị, cấu hình Phần mềm.	a) Có giao diện quản lý tài khoản người sử dụng.	x
		b) Yêu cầu xác thực người sử dụng khi truy cập quản trị, cấu hình Phần mềm.	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin
			2
		c) Yêu cầu xác thực người sử dụng khi truy cập sử dụng Phần mềm.	x
1.2	Có chức năng cho phép lưu trữ có mã hóa thông tin xác thực hệ thống.	Thông tin xác thực được lưu trữ có mã hóa trên Phần mềm sử dụng thuật toán hash từ SHA-256, SHA-512, SHA-3 và các thuật toán tương đương	x
1.3	Có chức năng cho phép thiết lập chính sách mật khẩu người sử dụng.	a) Có chức năng yêu cầu người dùng đặt mật khẩu mới khi đăng nhập lần đầu sử dụng mật khẩu mặc định.	x
		b) Có chức năng cho phép thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.	x
		c) Có chức năng cho phép thiết lập thời gian yêu cầu thay đổi mật khẩu.	x
		d) Có chức năng cho phép thiết lập thời gian mật khẩu hợp lệ.	x
		đ) Khóa tài khoản và yêu cầu nhập mật khẩu mới khi mật khẩu của tài khoản đó hết hạn thời gian hợp lệ.	x
		e) Mở khóa tài khoản khi thay đổi mật khẩu thành công đối với trường hợp mật khẩu hết hạn thời gian hợp lệ.	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin
			2
1.4	Có chức năng cho phép hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định.	a) Có giao diện cho phép thiết lập chính sách về giới hạn số lần đăng nhập sai trong khoảng thời gian nhất định.	x
		b) Có chức năng cảnh báo tới người sử dụng khi vi phạm chính sách.	x
		c) Có chức năng tự động ngăn cản việc đăng nhập tự động khi vi phạm chính sách trên.	x
2	Kiểm soát truy cập		
2.1	Có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout).	a) Có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi Phần mềm không nhận được yêu cầu từ người dùng.	x
		b) Hiển thị thông báo, đóng phiên kết nối đã hết hạn thời gian timeout và yêu cầu đăng nhập lại.	x
2.2	Có chức năng cho phép giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa.	a) Có giao diện cho phép quản trị viên quản lý chính sách về giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa.	x
		b) Có chức năng thực thi chính sách về giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa ở trên.	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin
			2
3	Nhật ký hệ thống		
3.1	Có chức năng cho phép ghi nhật ký hệ thống gồm những thông tin.	a) Phần mềm cung cấp chức năng ghi nhật ký hệ thống.	x
4	An toàn ứng dụng và mã nguồn		
4.1	Có chức năng cho phép kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý.	Có chức năng thực thi việc kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý	x
4.4	Có chức năng cho phép bảo đảm không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.	a) Thông tin xác thực, bí mật không được đưa trực tiếp vào mã nguồn ứng dụng mà phải được thiết lập thông qua giao diện cấu hình hệ thống.	x

e) Đánh giá điểm yếu và kiểm thử xâm nhập hạ tầng CNTT

- Sử dụng thông tin thu thập được để kiểm thử xâm nhập vào máy chủ, CSDL, container trong cụm Kubernetes theo khối lượng dự kiến tại tiểu mục 2.2 mục 2 Chương V E-HSMT.

- Tìm kiếm, phân tích các lỗ hổng hệ điều hành máy chủ, CSDL, image trong container, dịch vụ container runtime và các dịch vụ/ứng dụng khác (nếu có).

- Thực hiện tấn công thử nghiệm xâm nhập (pentest).

f) Tổng hợp và lập báo cáo đánh giá ANM&ATTT

Tổng hợp và lập báo cáo đánh giá ANM&ATTT, bao gồm nhưng không giới hạn các nội dung sau:

- Tổng hợp các lỗ hổng phát hiện được. Các lỗ hổng bảo mật phát hiện được sẽ được phân loại theo mức độ rủi ro: Nghiêm trọng, Cao, Trung Bình và Thấp.

- Liệt kê nội dung công việc, quá trình đánh giá. Các bước tiến hành thực hiện, cách thức thực hiện, phương pháp và công cụ sử dụng... đều được miêu tả chi tiết trong phần này của báo cáo.

- Mô tả chi tiết các lỗ hổng bảo mật phát hiện được trên hệ thống. Kèm theo

đó là hình ảnh minh họa cách thức khai thác, kết quả quá trình đánh giá.

- Đề xuất các phương án, giải pháp để EVNICT khắc phục các lỗ hổng bảo mật được phát hiện trên các hệ thống

3.2.4. Tái đánh giá ANM&ATTT và báo cáo tái đánh giá kết quả khắc phục lỗ hổng

Báo cáo kết quả tái đánh giá (kèm theo đó là hình ảnh minh họa) và đưa ra khuyến nghị giải pháp tiếp tục khắc phục, xử lý đối với các lỗ hổng còn tồn tại/chưa xử lý thành công (nếu có).

3.3. Tiến độ thực hiện

Nhà thầu phải có bảng tiến độ triển khai hợp lý, khả thi, phù hợp với giải pháp kỹ thuật, biện pháp tổ chức cung cấp dịch vụ và đáp ứng tiến độ thực hiện sau:

- Thời gian nhà thầu khảo sát, xây dựng kế hoạch kiểm tra đánh giá ANM&ATTT hệ thống thông tin và hoàn thành Phương án triển khai kiểm tra, đánh giá ANM&ATTT: trong vòng 7 ngày kể từ ngày Bên A có văn bản thông báo thực hiện hợp đồng.

- Thời gian nhà thầu đánh giá ANM&ATTT hệ thống: 43 ngày kể từ ngày Bên A thông qua phương án triển khai hợp đồng

- Thời gian chủ đầu tư khắc phục lỗ hổng (nếu có): 30 ngày kể từ khi Báo cáo đánh giá ANM&ATTT và khuyến nghị khắc phục các lỗ hổng bảo mật được Bên A thông qua.

- Thời gian nhà thầu tái đánh giá ANM&ATTT: 10 ngày kể từ khi Bên A thông báo Bên B vào tái đánh giá.

3.4. Tính hợp lệ của dịch vụ cung cấp

Nhà thầu có giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng do cơ quan nhà nước có thẩm quyền cấp, trong đó có cấp phép cho dịch vụ: dịch vụ kiểm tra, đánh giá an toàn thông tin mạng hoặc Có giấy chứng nhận đăng ký hoạt động hoặc có chức năng nhiệm vụ do cơ quan quản lý nhà nước có thẩm quyền cấp/giao trong lĩnh vực cung cấp dịch vụ an toàn thông tin mạng. Các giấy phép còn hiệu lực trong thời gian cung cấp dịch vụ.

3.5. Yêu cầu về năng lực và kinh nghiệm của nhân sự chủ chốt

- Yêu cầu chung: Hợp đồng lao động với nhân sự của nhà thầu, hoặc cam kết của nhân sự thực hiện, hoặc tài liệu khác tương đương trong trường hợp sử dụng một số nhân sự chủ chốt không thuộc quản lý của nhà thầu.

- Yêu cầu chi tiết:

STT	Vị trí công việc	Số lượng	Kinh nghiệm trong các công việc tương tự	Tài liệu chứng minh
1	Kỹ sư bậc 1	03	<ul style="list-style-type: none"> - Có tối thiểu 01 năm kinh nghiệm trong công việc kiểm thử xâm nhập (pentest). 	<ul style="list-style-type: none"> - Bằng cấp chuyên ngành theo yêu cầu Bảng số 02 mục 2 Chương III và đã sở hữu bằng này tối thiểu 01 năm tính đến thời điểm nộp hồ sơ. - Lý lịch của chuyên gia kê khai trên hệ thống theo mẫu số 06B và 06C Chương IV, trong đó mô tả rõ quá trình công tác theo trình tự thời gian liên tục, nêu cụ thể lĩnh vực chuyên môn chính, vai trò kỹ thuật thực tế, phạm vi công việc kiểm thử xâm nhập (pentest) đã tham gia. - Quá trình công việc được xác nhận bởi chủ đầu tư, hoặc đơn vị có hệ thống được đánh giá, hoặc thủ trưởng đơn vị đối với các đơn vị có chức năng nhiệm vụ do cơ quan quản lý nhà nước có thẩm quyền cấp/giao trong lĩnh vực cung cấp dịch vụ an toàn thông tin mạng.
			<ul style="list-style-type: none"> - Hoặc đã tham gia ít nhất 01 dự án/hợp đồng dịch vụ kiểm thử xâm nhập (pentest). 	<ul style="list-style-type: none"> - Bằng cấp chuyên ngành theo yêu cầu Bảng số 02 mục 2 Chương III và đã sở hữu bằng này tối thiểu 01 năm tính đến thời điểm nộp hồ sơ. - Lý lịch của chuyên gia kê khai trên hệ thống theo mẫu số 06B và 06C Chương IV. - Hợp đồng/dự án/QĐ giao nhiệm vụ hoặc các tài liệu tương tự khác có xác nhận của chủ đầu tư chứng minh nhân sự đã tham gia cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng theo hình thức pentest, trong đó các hợp đồng/dự án tương tự phải có tính chất công việc và giá trị tương đương với gói thầu đang xét. - Tài liệu chứng minh sự hoàn thành hợp đồng/dự án (Biên bản

STT	Vị trí công việc	Số lượng	Kinh nghiệm trong các công việc tương tự	Tài liệu chứng minh
				<p>nghiệm thu/Biên bản thanh lý hoặc tài liệu khác tương đương).</p>
2	Kỹ sư bậc 2	04	<p>- Có tối thiểu 02 năm kinh nghiệm trong công việc kiểm thử xâm nhập (pentest).</p>	<ul style="list-style-type: none"> - Bằng cấp chuyên ngành theo yêu cầu Bảng số 02 mục 2 Chương III và đã sở hữu bằng này tối thiểu 03 năm tính đến thời điểm nộp hồ sơ. - Lý lịch của chuyên gia kê khai trên hệ thống theo mẫu số 06B và 06C Chương IV, trong đó mô tả rõ quá trình công tác theo trình tự thời gian liên tục, nêu cụ thể lĩnh vực chuyên môn chính, vai trò kỹ thuật thực tế, phạm vi công việc kiểm thử xâm nhập (pentest) đã tham gia. - Quá trình công việc được xác nhận bởi chủ đầu tư, hoặc đơn vị có hệ thống được đánh giá, hoặc thủ trưởng đơn vị đối với các đơn vị có chức năng nhiệm vụ do cơ quan quản lý nhà nước có thẩm quyền cấp/giao trong lĩnh vực cung cấp dịch vụ an toàn thông tin mạng.

STT	Vị trí công việc	Số lượng	Kinh nghiệm trong các công việc tương tự	Tài liệu chứng minh
			<ul style="list-style-type: none"> - Hoặc đã tham gia ít nhất 02 dự án/hợp đồng dịch vụ kiểm thử xâm nhập (pentest). 	<ul style="list-style-type: none"> - Bằng cấp chuyên ngành theo yêu cầu Bảng số 02 mục 2 Chương III và đã sở hữu bằng này tối thiểu 03 năm tính đến thời điểm nộp hồ sơ. - Lý lịch của chuyên gia kê khai trên hệ thống theo mẫu số 06B và 06C Chương IV. - Hợp đồng/dự án/QĐ giao nhiệm vụ hoặc các tài liệu tương tự khác có xác nhận của chủ đầu tư chứng minh nhân sự đã tham gia cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng theo hình thức pentest, trong đó các hợp đồng/dự án tương tự phải có tính chất công việc và giá trị tương đương với gói thầu đang xét. - Tài liệu chứng minh sự hoàn thành hợp đồng/dự án (Biên bản nghiệm thu/Biên bản thanh lý hoặc tài liệu khác tương đương).
3	Kỹ sư bậc 4	02	<ul style="list-style-type: none"> - Có tối thiểu 05 năm kinh nghiệm trong công việc kiểm thử xâm nhập (pentest). 	<ul style="list-style-type: none"> - Bằng cấp chuyên ngành theo yêu cầu Bảng số 02 mục 2 Chương III và đã sở hữu bằng này tối thiểu 10 năm tính đến thời điểm nộp hồ sơ. - Lý lịch của chuyên gia kê khai trên hệ thống theo mẫu số 06B và 06C Chương IV, trong đó mô tả rõ quá trình công tác theo trình tự thời gian liên tục, nêu cụ thể lĩnh vực chuyên môn chính, vai trò kỹ thuật thực tế, phạm vi công việc kiểm thử xâm nhập (pentest) đã tham gia. - Quá trình công việc được xác nhận bởi chủ đầu tư, hoặc đơn vị có hệ thống được đánh giá, hoặc thủ trưởng đơn vị đối với các đơn vị có chức năng nhiệm vụ do cơ quan quản lý nhà nước có thẩm quyền cấp/giao trong lĩnh

STT	Vị trí công việc	Số lượng	Kinh nghiệm trong các công việc tương tự	Tài liệu chứng minh
				vực cung cấp dịch vụ an toàn thông tin mạng.
			- Hoặc đã tham gia ít nhất 03 dự án/hợp đồng dịch vụ kiểm thử xâm nhập (pentest).	<ul style="list-style-type: none"> - Bằng cấp chuyên ngành theo yêu cầu Bảng số 02 mục 2 Chương III và đã sở hữu bằng này tối thiểu 10 năm tính đến thời điểm nộp hồ sơ. - Lý lịch của chuyên gia kê khai trên hệ thống theo mẫu số 06B và 06C Chương IV. - Hợp đồng/dự án/QĐ giao nhiệm vụ hoặc các tài liệu tương tự khác có xác nhận của chủ đầu tư chứng minh nhân sự đã tham gia cung cấp dịch vụ kiểm tra, đánh giá an toàn thông tin mạng theo hình thức pentest, trong đó các hợp đồng/dự án tương tự phải có tính chất công việc và giá trị tương đương với gói thầu đang xét. - Tài liệu chứng minh sự hoàn thành hợp đồng/dự án (Biên bản nghiệm thu/Biên bản thanh lý hoặc tài liệu khác tương đương).

3.6. Các yêu cầu chi tiết đối với bảo lãnh thực hiện hợp đồng

- Bảo đảm thực hiện hợp đồng phải được nộp lên Bên A trong vòng 05 ngày làm việc kể từ khi Bên B nhận được Thư chấp thuận E-HSDT và trao Hợp đồng.
- Hình thức bảo đảm thực hiện hợp đồng: nhà thầu cung cấp một bảo đảm thực hiện hợp đồng theo hình thức thư bảo lãnh do Ngân hàng hoặc tổ chức tín dụng hoạt động hợp pháp tại Việt Nam phát hành và phải là bảo đảm không hủy ngang, không có điều kiện (trả tiền khi có yêu cầu, theo Mẫu số 15 Chương VIII).
- Giá trị bảo đảm thực hiện hợp đồng: Trong quá trình thực hiện hợp đồng Bên B phải đảm bảo giá trị bảo đảm thực hiện hợp đồng là 5% giá trị của hợp đồng đối với mọi trường hợp.
- Hiệu lực của bảo đảm thực hiện hợp đồng: Bảo đảm thực hiện hợp đồng có hiệu lực kể từ ngày phát hành bảo lãnh hoặc ngày hợp đồng có hiệu lực (tùy điều kiện nào đến sau) cho đến hết ngày thứ 28 sau khi Bên B hoàn thành tất cả công việc của Hợp đồng. Trường hợp bảo đảm thực hiện hợp đồng hết hiệu lực trước

ngày quy định nêu trên nhưng Bên B vẫn chưa hoàn thành nghĩa vụ hợp đồng, Bên B sẽ chịu trách nhiệm gia hạn hiệu lực Bảo đảm thực hiện hợp đồng và thanh toán chi phí cho việc gia hạn này.

Trường hợp Bên B là nhà thầu liên danh thì từng thành viên phải nộp bảo đảm thực hiện hợp đồng cho Bên A, mức bảo đảm tương ứng với phần giá trị hợp đồng mà mỗi thành viên thực hiện. Nếu Liên danh có thỏa thuận nhà thầu đứng đầu liên danh nộp bảo đảm thực hiện hợp đồng thì nhà thầu đứng đầu liên danh nộp bảo đảm thực hiện hợp đồng với giá trị là 2% giá trị của hợp đồng cho Bên A và từng thành viên liên danh phải nộp bảo đảm thực hiện hợp đồng cho nhà thầu đứng đầu liên danh tương ứng với giá trị hợp đồng do mình thực hiện.

- Tịch thu bảo đảm thực hiện hợp đồng: Bên A có quyền tịch thu Bảo lãnh thực hiện hợp đồng trong các trường hợp sau:

- + Bên B từ chối thực hiện hợp đồng khi hợp đồng đã có hiệu lực;
- + Bên B vi phạm thỏa thuận trong hợp đồng;
- + Bên B thực hiện hợp đồng chậm tiến độ do lỗi của mình nhưng từ chối gia hạn hiệu lực của bảo đảm thực hiện hợp đồng;
- + Bên B không gia hạn bảo lãnh đúng hạn theo quy định của Hợp đồng.

- Nếu Bên B chưa hoàn thành nghĩa vụ hợp đồng tại thời điểm 28 ngày trước ngày Bảo đảm thực hiện hợp đồng hết hiệu lực thì Bên B phải gia hạn hiệu lực Bảo đảm thực hiện hợp đồng với giá trị, hiệu lực phù hợp với quy định như trên và nộp cho Bên A trước thời điểm hết hiệu lực của Bảo đảm thực hiện hợp đồng tối thiểu 21 ngày.

Mục 4. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận đáp ứng yêu cầu tại mục 3 Chương V của E-HSMT.
2. Kế hoạch công tác phù hợp giải pháp và phương pháp luận nhà thầu đề xuất và đáp ứng yêu cầu tiến độ tại tiêu mục 3.3 mục 3 Chương V của E-HSMT.

Mục 5. Quy định về kiểm tra, nghiệm thu sản phẩm:

Bên B bắt đầu thực hiện hợp đồng kể từ ngày Bên A có văn bản thông báo hệ thống đã sẵn sàng phục vụ đánh giá ANM&ATTT.

Trong vòng 7 ngày kể từ ngày Bên A thông báo hệ thống sẵn sàng cho đánh giá ANM&ATTT, Bên B thực hiện khảo sát thu thập thông tin, xây dựng kế hoạch kiểm tra đánh giá và hoàn thiện Phương án triển khai kiểm tra, đánh giá ANM&ATTT theo yêu cầu của hợp đồng nộp cho đầu mối phụ trách kỹ thuật của Bên A kiểm tra, rà soát trình Lãnh đạo Bên A phê duyệt/thông qua làm căn cứ thực hiện.

Trong vòng 43 ngày kể từ ngày kế hoạch kiểm tra đánh giá đã được Lãnh đạo Bên A thông qua, Bên B hoàn thành đánh giá ANM&ATTT cho hệ thống Nghiên cứu phụ tải; lập báo cáo đánh giá ANM&ATTT kết quả các lỗ hổng tồn tại và khuyến nghị khắc phục các lỗ hổng nộp cho đầu mối phụ trách kỹ thuật của Bên A kiểm tra, rà soát trình Lãnh đạo Bên A phê duyệt/thông qua. Đầu mối phụ trách kỹ thuật hai bên ký Biên bản bàn giao và nghiệm thu báo cáo đánh giá ANM&ATTT sau khi được Lãnh đạo hai bên phê duyệt.

Bên A tổ chức khắc phục các lỗ hổng trong vòng 30 ngày từ khi nhận được khuyến nghị khắc phục các lỗ hổng của Bên B đã được Lãnh đạo hai bên thông qua.

Trong vòng 10 ngày sau khi nhận được yêu cầu tái đánh giá của Bên A, Bên B tổ chức tái đánh giá và hoàn thiện báo cáo tái đánh giá ANM&ATTT kết quả khắc phục lỗ hổng, nộp cho đầu mối phụ trách kỹ thuật của Bên A kiểm tra, rà soát trình Lãnh đạo Bên A phê duyệt/thông qua. Đầu mối phụ trách kỹ thuật hai bên ký Biên bản bàn giao và nghiệm thu báo cáo tái đánh giá sau khi được Lãnh đạo hai bên phê duyệt.

Trong vòng 10 ngày kể từ khi Bên B hoàn thành toàn bộ công việc của hợp đồng, Đại diện Lãnh đạo hai bên ký Biên bản nghiệm thu khối lượng công việc và Biên bản nghiệm thu hợp đồng.