

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: Xây dựng cổng thông tin kết nối, chia sẻ dữ liệu dùng chung của EVN (EVN Data Exchange Portal - EVNDXP)
2. Giá trị dự toán: 4.801.131.018 VNĐ (Bằng chữ: Bốn tỷ tám trăm linh một triệu một trăm ba mươi một nghìn không trăm mười tám 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 05 năm 2026
 - Hoàn thành triển khai: Tháng 06 năm 2026
6. Phạm vi thực hiện:
7. Hệ thống gồm các chức năng tại bảng sau:

TT	Chức năng
1	Quản lý dịch vụ
1.1	Khai báo, cập nhật nhóm dịch vụ
1.2	Khai báo, cập nhật dịch vụ
1.3	Tra cứu dịch vụ
2	Giám sát vận hành
2.1	Giám sát kết nối
2.2	Giám sát dịch vụ
2.3	Gửi thông báo
3	Quản lý API
3.1	Khai báo, cập nhật ứng dụng
3.2	Khai báo, cập nhật cấu hình xác thực ứng dụng
3.3	Khai báo, cập nhật API
4	Báo cáo
4.1	Báo cáo tần suất truy cập
4.2	Báo cáo chất lượng dịch vụ

TT	Chức năng
4.3	Tổng hợp và lưu báo cáo theo user
5	Tích hợp
5.1	Tích hợp dịch vụ cung cấp thông tin NDXP
5.2	Tích hợp dịch vụ kết nối CSDLDC
5.3	Tích hợp dịch vụ kết nối Cơ sở dữ liệu quốc gia về đăng ký doanh nghiệp
5.4	Tích hợp dịch vụ cổng dịch vụ công quốc gia
6	Quản trị
6.1	Quản lý người dùng
6.2	Phân quyền
6.3	Quản lý danh mục
6.4	Thiết lập báo cáo
6.5	Quản lý phiên bản

8. Phạm vi triển khai: Triển khai tập trung tại EVN

9. 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 kế hoạch kiểm tra đánh giá
- Đánh giá điểm yếu và kiểm thử xâm nhập cho ứng dụng web theo OWASP và yêu cầu về an toàn cơ bản theo quyết định 742/QĐ-BTTTT ngày 22/04/2022
- Đánh giá ATTT cho API tại văn bản 555/QĐ-EVN ngày 09/02/2023 và OWASP
- Đánh giá điểm yếu mã nguồn ứng dụng theo OWASP
- Đánh giá ATTT máy chủ theo Quyết định số 1290/QĐ-EVN ngày 05/09/2022
- Tổng hợp và lập báo cáo đánh giá ATTT kết quả các điểm yếu/lỗ hổng tồn tại trên toàn hệ thống và khuyến nghị khắc phục các lỗ hổng
- Tái đánh giá và báo cáo tái đánh giá kết quả khắc phục điểm yếu/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 lập phương án kế hoạch đánh giá: 5 ngày
- Thời gian đánh giá an toàn thông tin: 55 ngày
- Thời gian khắc phục lỗ hổng (nếu có): 25 ngày
- Thời gian tái đánh giá an toàn thông tin: 10 ngày
- Thời gian nghiệm thu hợp đồng: 5 ngày

Mục 2. Mục tiêu công việc:

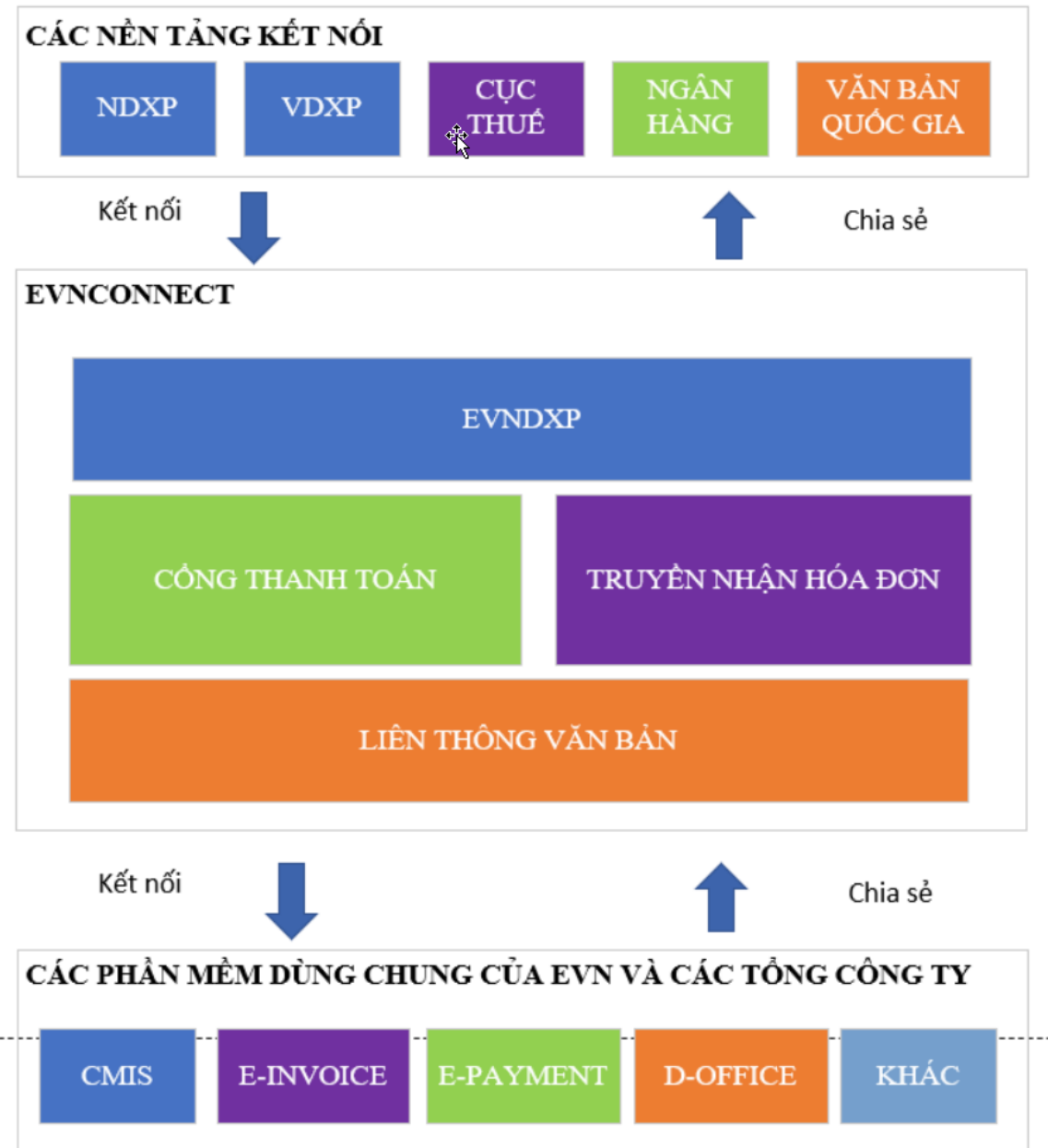
Đánh giá an toàn thông tin cho cổng kết nối, chia sẻ dữ liệu dùng chung của EVN (EVNDXP) nhằm phát hiện các lỗ hổng, điểm yếu của phần mềm, từ đó có giải pháp khắc phục lỗ hổng bảo mật nhằm ngăn chặn việc kẻ tấn công khai thác các lỗ hổng bảo mật đánh cắp dữ liệu, thay đổi hoặc mã hóa dữ liệu, chiếm quyền điều khiển hệ thống, gây tổn hại tới hệ thống CNTT của EVN.

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

Sau đây là thiết kế của cổng thông tin kết nối, chia sẻ dữ liệu dùng chung của EVN (EVN Data Exchange Portal - EVNDXP)

2.1. Thiết kế hệ thống phần mềm

2.1.1. Mô hình tổng quan hệ sinh thái EVNConnect



Mô hình thiết kế tổng thể

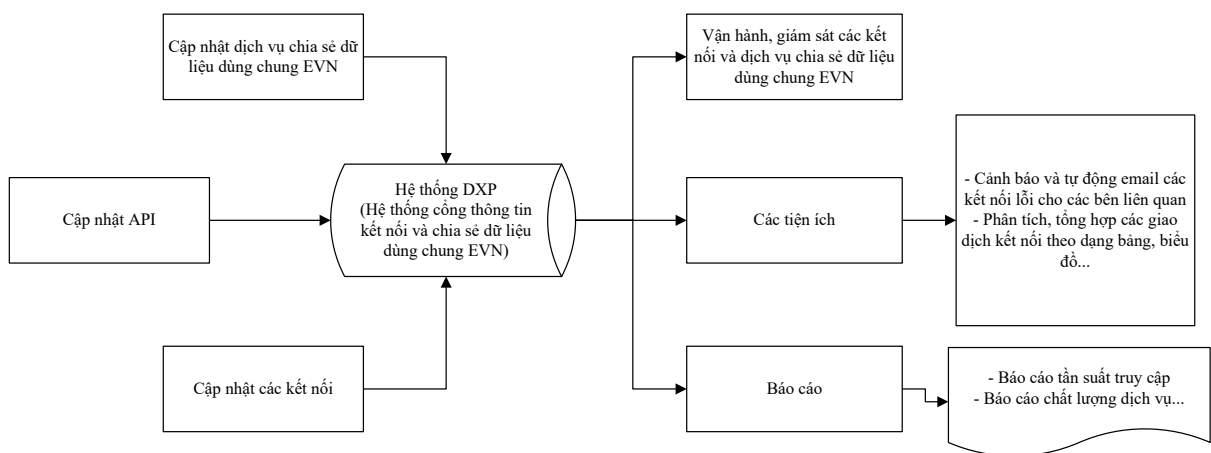
- Mô tả các thành phần
 - EVNDXP: Kết nối đến các nền tảng NDXP, VDXP
 - Công thanh toán:
 - Nhận yêu cầu chuyển tiền/yêu cầu tra soát giao dịch sang ngân hàng
 - Chủ động Vắn tin kết quả chuyển tiền/kết quả tra soát của ngân hàng
 - Nhận kết quả chuyển tiền/tra soát giao dịch của ngân hàng và trả kết quả cho các dịch vụ kết nối
 - Truyền nhận hóa đơn:
 - Truyền hóa đơn điện tử lên Cơ quan thuế
 - Nhận thông tin về tình trạng xử lý hóa đơn điện tử
 - Liên thông văn bản:

- Luồng gửi văn bản: EVN không gửi trực tiếp văn bản lên các Bộ/Ban/Ngành/các Tỉnh Văn bản từ hệ thống Doffice của EVN gửi lên trực UBQLV. Từ trực UBQLV vận hành sẽ gửi đến các nơi nhận tiếp theo.
- Luồng nhận văn bản: EVN lấy các văn bản được các Bộ/Ban/Ngành/các Tỉnh... có trên Trục UBQL với đơn vị nhận là EVN lấy về.

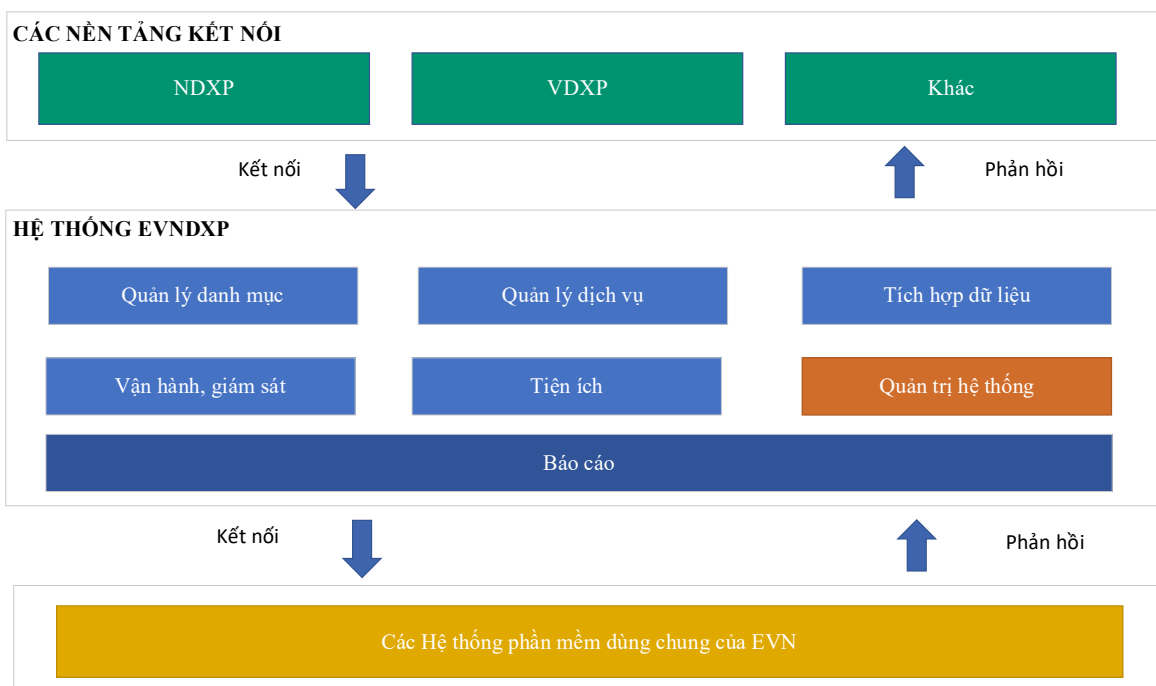
2.1.2. Mô hình tổng thể hệ thống

Hệ thống EVNDXP là cổng thông tin kết nối, chia sẻ dữ liệu dùng chung EVN. Hệ thống EVNDXP được tích hợp với các nền tảng, hệ thống CMIS, OMS, NDXP, VDXP, DVCQG

Mô hình nghiệp vụ EVNDXP



Sơ đồ liên kết EVNDXP với các các nền tảng, phần mềm khác



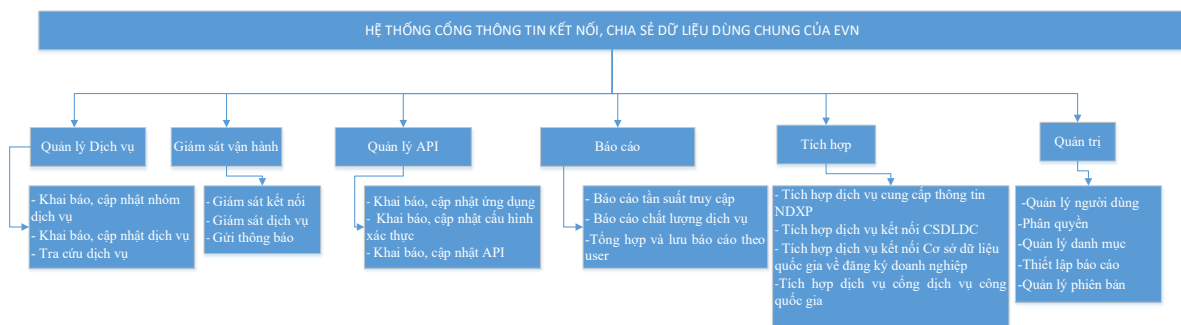
Phần mềm gồm các phân hệ:

1. Quản lý dịch vụ: quản lý, khai báo, cập nhật thông tin các dịch vụ EVN cung cấp và chia sẻ dữ liệu.
2. Giám sát vận hành: Giám sát kết nối, Giám sát dịch vụ, gửi thông báo,...
3. Quản lý API: Khai báo, cập nhật cấu hình xác thực, Khai báo, cập nhật API,...
4. Báo cáo: các báo cáo khai thác dữ liệu.
5. Tích hợp dữ liệu: tích hợp và chia sẻ các dữ liệu giữa EVN và các đối tác bên ngoài.
6. Quản trị: Chức năng quản lý người dùng, phân quyền

2.1.3 Phân tích và mô tả chức năng của phần mềm

a) Mô hình chức năng tổng thể

Hệ thống cổng thông tin kết nối, chia sẻ dữ liệu dùng chung của EVN (EVNDXP) bao gồm các chức năng chính sau:



b) Phân tích và mô tả chức năng

TT	Yêu cầu chức năng	Mô tả
1	Quản lý dịch vụ	
1.1	Khai báo, cập nhật nhóm dịch vụ	Chức năng khai báo, cập nhật nhóm dịch vụ: - Màn hình chính - Thêm, sửa, xóa nhóm dịch vụ
1.2	Khai báo, cập nhật dịch vụ	Chức năng khai báo, cập nhật dịch vụ: - Thêm, sửa, xóa dịch vụ - Hiện thị các tài khoản được phép truy cập dịch vụ
1.3	Tra cứu dịch vụ	Chức năng cho phép tra cứu dịch vụ
2	Giám sát vận hành	
2.1	Giám sát kết nối	Chức năng giám sát các dịch vụ kết nối tới: - Cơ sở dữ liệu dân cư - Cơ sở dữ liệu Quốc Gia về đăng ký doanh nghiệp - Cổng dịch vụ công Quốc Gia
2.2	Giám sát dịch vụ	Chức năng cho phép giám sát dịch vụ

TT	Yêu cầu chức năng	Mô tả
2.3	Gửi thông báo	Chức năng gửi thông báo về tình hình các dịch vụ
3	Quản lý API	
3.1	Khai báo, cập nhật ứng dụng	Chức năng khai báo, cập nhật ứng dụng
3.2	Khai báo, cập nhật cấu hình xác thực	Chức năng Khai báo, cập nhật cấu hình xác thực
3.3	Khai báo, cập nhật API	Chức năng Khai báo, cập nhật API
4	Báo cáo	
4.1	Báo cáo tần suất truy cập	Chức năng báo cáo tần suất truy cập <ul style="list-style-type: none"> - Theo tháng - Theo quý - Theo năm
4.2	Báo cáo chất lượng dịch vụ	Chức năng Báo cáo chất lượng dịch vụ <ul style="list-style-type: none"> - Theo tháng - Theo quý - Theo năm
4.3	Tổng hợp và lưu báo cáo theo user	Chức năng tổng hợp và lưu báo cáo theo user
5	Tích hợp	
5.1	Tích hợp dịch vụ cung cấp thông tin NDXP	Chức năng Tích hợp dịch vụ cung cấp thông tin NDXP <ul style="list-style-type: none"> - Upload hình ảnh sổ hộ khẩu, CCCD - Tra cứu chỉ số hóa đơn - Tra cứu tiền độ cấp điện - Thông tin cắt điện - Thông tin tiêu thụ điện tỉnh
5.2	Tích hợp dịch vụ kết nối CSDLDC	Chức năng Tích hợp dịch vụ kết nối CSDLDC <ul style="list-style-type: none"> - Tra cứu thông tin cư dân - Xác thực thông tin chứng minh thư nhân dân/căn cước công dân - Xác thực chủ hộ
5.3	Tích hợp dịch vụ kết nối Cơ sở dữ liệu quốc gia về đăng ký doanh nghiệp	Chức năng tích hợp dịch vụ kết nối Cơ sở dữ liệu quốc gia về đăng ký doanh nghiệp Tra cứu thông tin doanh nghiệp
5.4	Tích hợp dịch vụ cổng dịch vụ công quốc gia	Chức năng tích hợp dịch vụ cổng dịch vụ công quốc gia: <ul style="list-style-type: none"> - Đồng bộ hồ sơ lên Cổng DVCQG - Cập nhật trạng thái hồ sơ lên Cổng DVCQG - Tra cứu hóa đơn Cổng DVCQG - Thông tin file hóa đơn tiền điện Cổng DVCQG

TT	Yêu cầu chức năng	Mô tả
		<ul style="list-style-type: none"> - Thông tin kết quả thanh toán Cổng DVCQG - Tích hợp với Trung tâm dữ liệu Quốc Gia - Chia sẻ file hồ sơ giấy tờ
6	Quản trị	
6.1	Quản lý người dùng	Chức năng quản lý người dùng: <ul style="list-style-type: none"> - Khai báo người dùng - Đổi mật khẩu
6.2	Phân quyền	Chức năng phân quyền <ul style="list-style-type: none"> - Quản lý chức năng - Phân quyền chức năng
6.3	Quản lý danh mục	Chức năng quản lý danh mục <ul style="list-style-type: none"> - Danh mục Đơn vị - Các danh mục dùng chung
6.4	Thiết lập báo cáo	Chức năng Thiết lập báo cáo Mẫu báo cáo (templtae) <ul style="list-style-type: none"> - Tham số báo cáo
6.5	Quản lý phiên bản	Chức năng Quản lý phiên bản Xem phiên bản

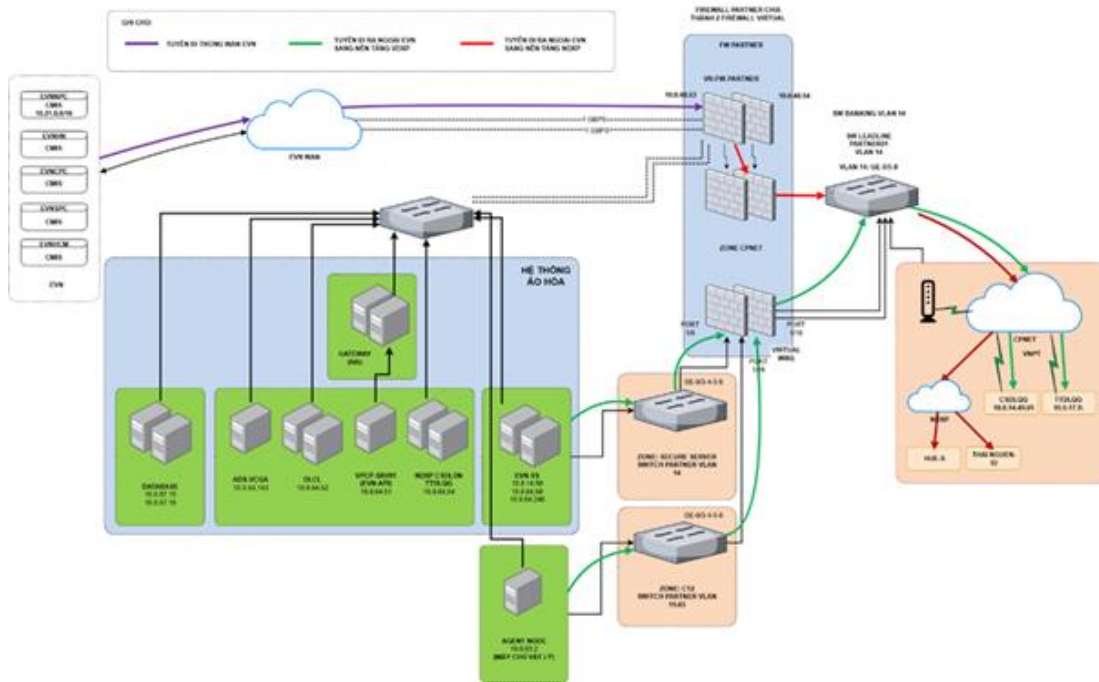
2.1.4. Thiết kế cơ sở dữ liệu

STT	Danh sách bảng
I	QUẢN LÝ DANH MỤC
1	Danh mục Enum API
2	Danh mục loại xác thực
3	Danh mục điều hướng
4	Danh mục tổ chức
5	Danh mục đơn vị hành chính
II	DỊCH VỤ CÔNG
6	Hồ sơ tệp tin
7	Hồ sơ dịch vụ công
8	Loại yêu cầu thủ tục hành chính
9	Loại giấy tờ
10	Tiến trình xử lý hồ sơ
11	Thành phần hồ sơ
III	QUẢN TRỊ HỆ THỐNG
12	Chức năng hệ thống
13	Lịch sử đăng nhập/đăng xuất
14	Phân quyền role cho tổ chức
15	Phân quyền user cho tổ chức
16	Phân quyền chức năng theo role

17	Phân quyền chức năng theo user
18	Quản lý refresh token
19	Role
20	User
21	Thiết bị user
22	Nhật ký user
23	Quan hệ phân quyền role-user
24	Tham số hệ thống
25	Bảng message EVNDXP
IV	QUẢN TRỊ CẤU HÌNH API, DỊCH VỤ
26	Chi tiết log API
27	Tổng hợp log API
28	Ứng dụng
29	API của ứng dụng
30	Tham số API ứng dụng
31	Cấu hình xác thực API ứng dụng
32	Cấu hình xác thực
33	Thông tin xác thực
34	Nhóm ứng dụng
35	Trích xuất tham số ứng dụng
36	Dịch vụ
37	Mapping API – Dịch vụ
38	Nhóm dịch vụ
39	Chi tiết log dịch vụ
40	Log dịch vụ max
41	Tổng hợp log dịch vụ
V	TRUNG TÂM DỮ LIỆU QUỐC GIA
42	Dữ liệu đồng bộ hợp đồng cá nhân
43	Dữ liệu đồng bộ hợp đồng tổ chức

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: vùng máy chủ nội bộ, nơi đặt các máy chủ SS tạo kết nối tới cổng DVCQG. Vùng này được bảo vệ bởi 1 cặp thiết bị Firewall Palo Alto PA3440 chạy HA.

Vùng mạng WAN: đây là 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.

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

• **Danh mục các thiết bị/máy chủ phục vụ hệ thống:**

- Máy chủ dưới đây sẽ được cấp phát và khai thác trên nền tảng hệ thống ảo hóa và lưu trữ hiện hữu tại EVNICT. Các máy chủ ảo hóa này sẽ được cấp phát ở phân vùng Máy chủ ảo hóa, được giám sát trên hệ thống Giám sát của EVNICT, ngoài ra toàn bộ các máy chủ trong cổng dịch kết nối cũng hiện đang được giám sát trên hệ thống hostmonitor tại NOC. Phân vùng mạng chủ yếu của công dịch vụ EVNDXP hiện thuộc dải mạng đã được quy hoạch là VLAN (dải mạng cho các máy chủ Partner) hệ thống hiện được sizing và cấp phát theo nhu cầu thực tế sử dụng.

- Bổ sung thêm cặp máy chủ Gateway (02 máy chủ) đóng vai trò điều phối, cân bằng tải và quản lý truy cập hệ thống, các máy chủ API VDXP, API NDXP, Database cũng như EVN-SS sẽ được cấp thêm 01 máy chủ dự phòng chạy theo cơ chế HA cân bằng tải.

Hệ thống về cơ bản được cài đặt agent và cấu hình sao lưu trên các hệ thống sao lưu chuyên dụng và hệ thống NAS tại ICT theo quy định của ICT, tuy nhiên do ICT hiện chưa hoàn thiện giải pháp sao lưu 3-2-1, do đó việc sao lưu theo đúng chủ trương của chính phủ cũng như EVN sẽ được hoàn thiện khi phần mô hình này được mua sắm và đầy đủ trong thời gian tới. Tuy nhiên phần sao lưu dữ liệu / cấu hình hệ thống hiện đang được sao lưu đầy đủ trên local máy chủ, hệ thống sao lưu chuyên dụng và hệ thống sao lưu file system EVNNAS.

STT	Tên thiết bị/ phần mềm	Số lượng	Mô tả/ Mục đích sử dụng	Thông số kỹ thuật và các tiêu chuẩn (tối thiểu)	Ghi chú
1	Máy chủ Gateway	02	Đóng vai trò điều phối, cân bằng tải và quản lý truy cập hệ thống	- CPU: ≥ 16 core, 2.4GHz - RAM: \geq 32GB - Ổ cứng: \geq 150GB	Chính + Dự phòng
2	Máy chủ APP (Web, API)	01	Lưu trữ và vận hành các ứng dụng dịch vụ: CMS, xử lý logic nghiệp vụ và giao tiếp với DB cũng như Gateway.	- CPU: ≥ 32 core, 2.4GHz trở lên - RAM: \geq 64GB - Ổ cứng: \geq 500GB	
3	Máy chủ API VDXP	02	Giao tiếp với nền tảng VDXP	- CPU: ≥ 24 core, 2.4GHz trở lên - RAM: ≥ 16 GB - Ổ cứng: \geq 500GB	Chính + Dự phòng
4	Máy chủ API NDXP	02	Giao tiếp với nền tảng NDXP	- CPU: ≥ 24 core, 2.4GHz trở lên - RAM: ≥ 16 GB - Ổ cứng: \geq 500GB	Chính + Dự phòng
5	Máy chủ DB	02	Lưu trữ cơ sở dữ liệu hệ thống; DB Backup phục vụ dự phòng và khôi phục dữ	- CPU: ≥ 32 core, 2.4GHz trở lên - RAM: ≥ 64 GB - Ổ cứng: \geq 500GB	Chính + Dự phòng + Backup

STT	Tên thiết bị/ phần mềm	Số lượng	Mô tả/ Mục đích sử dụng	Thông số kỹ thuật và các tiêu chuẩn (tối thiểu)	Ghi chú
			liệu khi có sự cố.		
6	Máy chủ EVN-SS	02	Giao tiếp với nền tảng NDXP	Máy chủ ảo - CPU: 4 Core - Ram: 8 GB - HDD: 160 GB + 400GB - OS: Ubuntu Server 64bit	Đảm bảo kết nối hạ tầng từ EVN sang CPNET và ngược lại.
7	VCGA	01	Máy chủ ký số Ban cơ yếu	Máy chủ ảo: - HĐH: Linux 9 - CPU: 16 Cores - RAM: 32 GB - HDD: 500GB	Application partner

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

TT	Tên thiết bị	Mô tả	Diễn giải	Ghi chú
1	FW-PARTNER-01	Cấp thiết bị firewall Palo Alto	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-PARTNER-02			
3	TOR106-SW-PARTNER01	Thiết bị switch Juniper	Switch dùng chung, cung cấp các kết nối mạng cho các máy chủ, thiết bị tại vùng mạng Partner (chạy chế độ Stack).	DC 11 Cửa Bắc
4	TOR106-SW-PARTNER02			

2.3. Cấp độ an toàn thông tin

Cổng thông tin kết nối, chia sẻ dữ liệu dùng chung của EVN đáp ứng nhu cầu quản lý các dịch vụ kết nối, chia sẻ dữ liệu giữa EVN và ngoài EVN, cụ thể:

- Thông tin được xử lý thông qua hệ thống thông tin được phân loại theo thuộc tính bí mật, căn cứ khoản 1, Điều 6, Nghị định 85/2016/NĐ-CP:

- + Có xử lý thông tin riêng;
- + Có xử lý thông tin cá nhân;

- + Không xử lý thông tin bí mật nhà nước.
- Phân loại hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của các cơ quan, tổ chức trong phạm vi một ngành, một tỉnh hoặc một số tỉnh.
- + Hệ thống cung cấp dịch vụ kết nối với các nền tảng ngoài EVN.
- Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của các cơ quan, tổ chức trong phạm vi toàn ngành EVN, các Bộ/Ban/Ngành/các Tỉnh.... Căn cứ theo quy định khoản 3 Điều 9 Nghị định 85/2016/NĐ-CP, Hệ thống được đề xuất cấp độ 3.

Mục 3. Yêu cầu kỹ thuật của gói thầu:

3.1. Phạm vi cung cấp dịch vụ

▪ ***Công việc 1: Khảo sát thu thập thông tin và xây dựng kế hoạch kiểm tra đánh giá;***

▪ ***Công việc 2: Đánh giá ATTT hệ thống gồm:***

- Đánh giá điểm yếu và kiểm thử xâm nhập cho ứng dụng web theo OWASP và yêu cầu về an toàn cơ bản theo quyết định 742/QĐ-BTTTT ngày 22/04/2022.
- Đánh giá ATTT cho API tại văn bản 555/QĐ-EVN ngày 09/02/2023 và OWASP
- Đánh giá điểm yếu mã nguồn ứng dụng theo OWASP
- Đánh giá ATTT máy chủ theo Quyết định số 1290/QĐ-EVN ngày 05/09/2022
- Tổng hợp và lập báo cáo đánh giá ATTT kết quả các điểm yếu/lỗ hổng tồn tại trên toàn hệ thống và khuyến nghị khắc phục các lỗ hổng

▪ ***Công việc 3: Tái đánh giá và báo cáo tái đánh giá kết quả khắc phục điểm yếu/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, thử nghiệm xâm nhập được cung cấp đầy đủ thông tin cũng như đặc quyền đối với hệ thống.

3.2.2. Nội dung đánh giá an toàn thông tin

a) Khảo sát thu thập thông tin và xây dựng kế hoạch kiểm tra đánh giá

- Khảo sát thiết kế
- Khảo sát ứng dụng
- Khảo sát hạ tầng CNTT

- Lập kế hoạch kiểm tra và đánh giá

b) Thực hiện đánh giá ATTT

b.1) Đánh giá điểm yếu và kiểm thử xâm nhập cho ứng dụng web theo OWASP và yêu cầu về an toàn cơ bản theo quyết định 742/QĐ-BTTTT ngày 22/04/2022.

- 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 3**:

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
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	x	x	x	x
		b) Yêu cầu xác thực người sử dụng khi truy cập quản trị, cấu hình Phần mềm.	x	x	x	x	x
		c) Yêu cầu xác thực người sử dụng khi truy cập sử dụng Phần mềm.	x	x	x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
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	x	x	x	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	x	x	x	x
		b) Có chức năng cho phép thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.	x	x	x	x	x
		c) Có chức năng cho phép thiết lập thời gian yêu cầu thay đổi mật khẩu.		x	x	x	x
		d) Có chức năng cho phép thiết lập thời gian mật khẩu hợp lệ.		x	x	x	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	x	x	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	x	x	x
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	x	x	x
		b) Có chức năng cảnh báo tới người sử dụng khi vi phạm chính sách.		x	x	x	x
		c) Có chức năng tự động ngăn cản việc đăng nhập tự động khi vi phạm chính sách trên.		x	x	x	x
		đ) Có chức năng tự động vô hiệu hóa tài khoản nếu vi phạm chính sách trên.			x	x	x
1.5	Có chức năng cho phép mã hóa thông tin xác thực	Chức năng bảo đảm mật khẩu được mã hóa trước khi gửi qua môi trường mạng.			x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
	trước khi gửi qua môi trường mạng.						
1.6	Có chức năng cho phép sử dụng cơ chế xác thực đa nhân tố để xác thực người sử dụng.	a) Có giao diện cho phép quản trị viên quản lý chính sách về xác thực đa nhân tố.				X	X
		b) Tích hợp các bước xác thực đa nhân tố khi chính sách đối với trường hợp này được kích hoạt.				X	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	X	X	X	X
		b) Hiện thị thông báo, đóng phiên kết nối đã hết hạn thời gian timeout và yêu cầu đăng nhập lại.		X	X	X	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	X	X	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	X	X	X
2.3	Có chức năng cho phép phân quyền và cấp quyền tối thiểu truy cập, quản trị, sử dụng tài nguyên khác nhau của Phần mềm với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau.	a) Có giao diện cho phép quản trị viên quản lý chính sách về phân quyền tài khoản theo từng nhóm tài khoản.			X	X	X
		b) Phân loại nhóm tài khoản theo ít nhất 03 nhóm:			X	X	X
		i. Tài khoản người sử dụng thông thường;					
		ii. Tài khoản quản trị mức sử dụng;					

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		iii. Tài khoản quản trị mức phát triển, vận hành.					
		c) Có chức năng thực thi chính sách phân quyền và cấp quyền tối thiểu truy cập, quản trị, sử dụng tài nguyên khác nhau ở trên.			x	x	x
2.4	Có chức năng cho phép thiết lập quyền tối thiểu (quyền truy cập, quản trị) cho tài khoản quản trị ứng dụng theo quyền hạn.	a) Có giao diện cho phép quản trị viên thiết lập quyền cho các tài khoản.			x	x	x
		b) Có chức năng thực thi chính sách phân quyền cho các tài khoản ở trên.			x	x	x
2.5	Có chức năng cho phép thay đổi, tách biệt công quản trị ứng dụng với công cung cấp dịch vụ ứng dụng.	c) Có giao diện cho phép quản trị viên quản lý chính sách về công quản trị ứng dụng và công cung cấp dịch vụ ứng dụng.					x
		b) Có chức năng thực thi chính sách tách biệt công quản trị ứng dụng với công cung cấp dịch vụ ứng dụng ở trên.					x
2.6	Có chức năng cho phép khóa tạm thời quản trị ứng dụng trong khoảng thời gian ngoài giờ làm việc.	a) Có giao diện cho phép quản trị viên quản lý chính sách về khoảng thời gian được phép thực hiện thao tác quản trị.					x
		b) Có chức năng thực thi chính sách về khoảng thời gian được phép thực hiện thao tác quản trị hệ thống ở trên.					x
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	x	x	x	x
		b) Nhật ký hệ thống được phân loại theo ít nhất 05 nhóm:			x	x	x
		i. Nhật ký truy cập Phần mềm;					
		ii. Nhật ký đăng nhập khi quản trị Phần mềm;					

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		iii. Nhật ký các lỗi phát sinh trong quá trình hoạt động; iv. Nhật ký quản lý tài khoản; v. Nhật ký thay đổi cấu hình Phần mềm					
3.2	Có chức năng cho phép quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung.	a) Có giao diện cho phép quản trị viên quản lý chính sách về nhật ký hệ thống.			x	x	x
		b) Cho phép quản trị viên cấu hình khoảng thời gian lưu trữ nhật ký qua giao diện trên.			x	x	x
		c) Lưu trữ nhật ký với ít nhất 05 thông tin:			x	x	x
		i. Thời điểm sinh nhật ký;					
		ii. Phân nhóm nhật ký;					
3.3	Có chức năng cho phép phân quyền truy cập, quản lý dữ liệu nhật ký hệ thống đối với các tài khoản có chức năng quản trị hệ thống khác nhau.	iii. Mô tả thao tác/lỗi;					
		iv. Đối tượng thực hiện thao tác/sinh lỗi;					
		v. Mức độ quan trọng.					
3.3		a) Có giao diện cho phép quản trị viên quản lý chính sách về phân quyền tài khoản theo từng nhóm tài khoản quản trị.					x
		b) Có chức năng thực thi chính sách phân quyền ở trên.					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	x	x	x	x
4.2	Có chức năng cho phép bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF	Phần mềm được kiểm tra, đánh giá, kiểm thử xâm nhập theo tiêu chuẩn OWASP và không tồn tại điểm yếu cho phép kẻ tấn công khai thác thông qua các dạng tấn công: SQL Injection, OS command			x	x	x

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		injection, RFI, LFI, Xpath Injection, XSS, CSRF.					
4.3	Có chức năng cho phép kiểm soát lỗi, thông báo lỗi từ ứng dụng.	a) Có chức năng kiểm soát lỗi, chỉ hiển thị các thông báo lỗi được kiểm soát đến người dùng và không hiển thị các lỗi bên trong hệ thống.			X	X	X
		b) Có chức năng hiển thị thông báo lỗi đến người sử dụng.			X	X	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	X	X	X
5. Bảo mật thông tin liên lạc							
5.1	Có chức năng cho phép mã hóa thông tin, dữ liệu trước khi truyền đưa, trao đổi qua môi trường mạng (đôi với các ứng dụng yêu cầu sử dụng chữ ký số).	Có chức năng cho phép mã hóa dữ liệu trước khi truyền đưa, trao đổi qua môi trường mạng sử dụng chữ ký số.			X	X	X
6. Sao lưu dự phòng							
6.1	Có chức năng cho phép tự động sao lưu dự phòng.	a) Có giao diện cho phép quản trị viên thiết lập chính sách về sao lưu dự phòng cơ sở dữ liệu và cấu hình hệ thống.			X	X	X
		b) Có chức năng cho phép thực hiện việc sao lưu dự phòng theo chính sách ở trên.			X	X	X
6.2	Có chức năng cho phép phép gán nhãn loại dữ liệu được lưu trữ theo quy tắc được thiết lập.	a) Có giao diện cho phép quản trị viên quản lý chính sách về phân loại dữ liệu được lưu trữ theo từng nhóm dữ liệu.				X	X
		b) Có chức năng cho phép lưu trữ dữ liệu theo tên định dạng đối với từng loại dữ liệu tại mục trên.				X	X
6.3	Có chức năng cho phép thiết lập cấu hình để gửi dữ liệu dự phòng về hệ thống lưu trữ tập trung.	a) Có giao diện cho phép quản trị viên thiết lập cấu hình để gửi dữ liệu dự phòng về hệ thống lưu trữ tập trung.					X

TT	Yêu cầu kỹ thuật	Mô tả yêu cầu	Cấp độ của hệ thống thông tin				
			1	2	3	4	5
		b) Có chức năng cho phép thực hiện sao lưu dự phòng thủ công cơ sở dữ liệu và cấu hình hệ thống lên hệ thống lưu trữ tập trung.					x
		c) Có chức năng cho phép thực hiện sao lưu dự phòng tự động cơ sở dữ liệu và cấu hình hệ thống lên hệ thống lưu trữ tập trung.					x
		d) Có chức năng cho phép khôi phục dữ liệu, cấu hình hệ thống từ dữ liệu được lưu trữ trên hệ thống lưu trữ tập trung.					x

b.2) Đánh giá ATTT cho API văn bản 555/QĐ-EVN ngày 09/02/2023 và OWASP

- 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

câu 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; - 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

STT	Yêu cầu đảm bảo ATTT cho các API
	nhạy cảm, không cần thiết.
4	<p><i>Mass Assignment - Kiểm tra các dữ liệu cập nhật</i></p> <p>a. Mục đích: kiểm soát các trường thông tin cập nhật và hệ thống</p> <p>b. Các yêu cầu và khuyến nghị:</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 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>

STT	Yêu cầu đảm bảo ATTT cho các API
	<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; - 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.

b.3) Đánh giá ATTT cho mã nguồn ứng dụng theo OWASP

- 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

b.4) Đánh giá ATTT máy chủ theo Quyết định số 1290/QĐ-EVN ngày 5/9/2022

- Dựa trên Quyết định số 1290/QĐ-EVN ngày 05/09/2022 của Tập đoàn Điện lực Việt Nam sẽ thực hiện đánh giá cho các máy chủ trong hệ thống theo từng loại đánh giá quy định tại chương III, IV.

- Chi tiết Quyết định 1290/QĐ-EVN ngày 5/9/2022 được mô tả phụ lục kèm

theo.

Ghi chú: *Số lượng máy chủ, loại đánh giá tạm tính trên cơ sở Danh mục thiết bị tại tiểu mục 2.2.2 Mục 2 Chương này, và sẽ được chuẩn xác sau khi ký hợp đồng, Nhà thầu thực hiện khảo sát để lập phương án, kế hoạch đánh giá.*

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 ATTT hệ thống thông tin và hoàn thành phương án triển khai hợp đồng: 5 ngày kể từ ngày Bên A có văn bản thông báo thực hiện hợp đồng.
- Thời gian nhà thầu đánh giá an toàn thông tin hệ thống: 55 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): 25 ngày kể từ khi Báo cáo đánh giá ATTT và khuyến nghị khắc phục các lỗ hổng bảo mật (nếu có) được Bên A thông qua.
- Thời gian nhà thầu tái đánh giá an toàn thông tin: 10 ngày kể từ khi Bên A thông báo Bên B vào tái đánh giá.
- Thời gian nghiệm thu: 5 ngày kể từ khi bên B hoàn thành toàn bộ công việc theo phạm vi hợp đồng.

Ghi chú: *Trên cơ sở thực tế khảo sát, thu thập thông tin để xây dựng kế hoạch kiểm tra đánh giá của nhà thầu, công việc đánh giá, tái đánh giá sẽ được bố trí thực hiện linh hoạt, không nhất thiết phải theo tuần tự để đảm bảo tiến độ thực hiện hợp đồng. Nội dung này sẽ được Hai Bên thống nhất cụ thể trong phương án, kế hoạch kiểm tra đánh giá tại thời điểm khảo sát.*

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

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 chuyên ngành CNTT hoặc ATTT; - Và đã tham gia ít nhất 01 dự án/hợp đồng dịch vụ kiểm tra, đánh giá an toàn thông tin mạng theo hình thức pentest 	<ul style="list-style-type: none"> - 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; - Bằng cấp chuyên ngành chuyên ngành ATTT hoặc CNTT theo yêu cầu - 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 đương 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. - 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).
2	Kỹ sư bậc 2	02	<ul style="list-style-type: none"> - Có tối thiểu 03 năm kinh nghiệm trong chuyên ngành CNTT hoặc ATTT - Và đã tham gia ít nhất 02 dự án/hợp đồng dịch vụ kiểm tra, đánh giá an toàn thông tin mạng theo hình thức pentest. 	<ul style="list-style-type: none"> - 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; - Bằng cấp chuyên ngành chuyên ngành ATTT hoặc CNTT theo yêu cầu - 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 đương 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

STT	Vị trí công việc	Số lượng	Kinh nghiệm trong các công việc tương tự	Tài liệu chứng minh
				- 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	01	<ul style="list-style-type: none"> - Có tối thiểu 09 năm kinh nghiệm trong chuyên ngành CNTT hoặc ATTT - Và đã tham gia ít nhất 03 dự án/hợp đồng dịch vụ kiểm tra, đánh giá an toàn thông tin mạng theo hình thức pentest 	<ul style="list-style-type: none"> - 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; - Bảng cấp chuyên ngành chuyên ngành ATTT hoặc CNTT theo yêu cầu - 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 đương 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 - 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 5% 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 tiểu 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 ATTT.

Trong vòng 5 ngày kể từ ngày Bên A thông báo hệ thống sẵn sàng cho đánh giá 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 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 55 ngày kể từ ngày kế hoạch kiểm tra đánh giá đã được Lãnh đạo Bên A thông qua, Bên B hoàn thành đánh giá an toàn thông tin cho hệ thống cơ sở dữ liệu môi trường của EVN; lập báo cáo đánh giá ATTT kết quả các điểm yếu/lỗ hổng tồn tại trên toàn hệ thống 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 ATTT sau khi được Lãnh đạo hai bên phê duyệt.

Bên A tổ chức khắc phục các lỗ hổng, điểm yếu (nếu có) trong vòng 25 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 an toàn thông tin kết quả khắc phục điểm yếu/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 5 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.