

BỘ Y TẾ
TRUNG TÂM THÔNG TIN
Y TẾ QUỐC GIA

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

Số: 379/TTYQG-ĐVCĐS

Hà Nội, ngày 20 tháng 4 năm 2026

V/v mời tham gia chỉ định thầu rút gọn
gói thầu “Nâng cấp Nền tảng Hỗ trợ tư vấn
khám, chữa bệnh từ xa (Nền tảng
VTelehealth)”

Kính gửi: Các đơn vị tham dự chỉ định thầu rút gọn

Căn cứ Quyết định số 2955/QĐ-BYT ngày 28/10/2022 của Bộ trưởng Bộ Y tế về việc ban hành Kế hoạch thúc đẩy phát triển và sử dụng các nền tảng số y tế, thực hiện Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030;

Căn cứ Quyết định số 823/QĐ-BYT ngày 15/02/2023 của Bộ Y tế phê duyệt kế hoạch triển khai nền tảng hỗ trợ tư vấn khám chữa bệnh từ xa năm 2023;

Căn cứ Hợp đồng tài trợ hoạt động khoa học và công nghệ số 10.2024/HĐTT/TTYQG-GOTRUST ngày 13/05/2024 giữa Trung tâm Thông tin y tế Quốc gia với Công ty Cổ phần Dịch vụ & Giải pháp công nghệ GOTRUST;

Căn cứ Phụ lục điều chỉnh thời gian thực hiện hợp đồng ngày 12/5/2025 giữa Trung tâm Thông tin y tế Quốc gia với Công ty Cổ phần Dịch vụ và Giải pháp công nghệ GOTRUST;

Căn cứ Quyết định số 124/QĐ-TTYQG ngày 15/4/2026 của Giám đốc Trung tâm Thông tin y tế Quốc gia về việc phê duyệt thuyết minh hoạt động và dự toán kinh phí Nâng cấp Nền tảng Hỗ trợ tư vấn khám, chữa bệnh từ xa (Nền tảng VTelehealth);

Căn cứ Quyết định số 132/QĐ-TTYQG ngày 20/4/2026 của Giám đốc Trung tâm Thông tin y tế Quốc gia về việc phê duyệt kế hoạch lựa chọn nhà thầu gói thầu “Nâng cấp Nền tảng Hỗ trợ tư vấn khám, chữa bệnh từ xa (Nền tảng VTelehealth)”.

Trung tâm Thông tin y tế Quốc gia đang tổ chức lựa chọn nhà thầu thực hiện gói thầu Nâng cấp Nền tảng Hỗ trợ tư vấn khám, chữa bệnh từ xa (Nền tảng VTelehealth) với hình thức lựa chọn nhà thầu là Chỉ định thầu rút gọn, thông tin cụ thể như sau:

1. Thông tin gói thầu:

- Tên gói thầu: Nâng cấp Nền tảng Hỗ trợ tư vấn khám, chữa bệnh từ xa (Nền tảng VTelehealth)

- Chủ đầu tư: Trung tâm Thông tin y tế Quốc gia

- Giá gói thầu: 294.600.000 đồng

- Nguồn vốn: Từ nguồn tài trợ theo Hợp đồng tài trợ hoạt động khoa học

và công nghệ số 10.2024/HĐTT/TTYQG-GOTRUST ngày 13/05/2024 giữa Trung tâm Thông tin y tế Quốc gia với Công ty Cổ phần Dịch vụ & Giải pháp công nghệ GOTRUST.

- Hình thức lựa chọn nhà thầu: Chỉ định thầu rút gọn.
- Loại hợp đồng: Hợp đồng trọn gói.
- Thời gian thực hiện hợp đồng: 16 ngày (kể từ ngày hợp đồng có hiệu lực).

2. Nội dung yêu cầu gói thầu: Tại phụ lục kèm theo

3. Yêu cầu nộp hồ sơ:

- Văn bản tham dự chỉ định thầu của đơn vị.
- Hồ sơ năng lực của đơn vị.

- Bảng giá dự thầu của đơn vị.

4. Thời gian nhận hồ sơ:

Từ ngày 20/04/2026 đến 17h30 ngày 21/04/2026

(Các hồ sơ nhận sau thời điểm này sẽ không được xem xét).

5. Hình thức nộp hồ sơ:

- Nộp trực tiếp tại địa chỉ: Bộ phận văn thư, Trung tâm Thông tin y tế Quốc gia, địa chỉ: Ngõ 135/1 Phố Núi Trúc, Phường Kim Mã, Thành phố Hà Nội

6. Tài liệu kèm theo:

- Quyết định số 132/QĐ-TTYQG ngày 20/04/2026 của Giám đốc Trung tâm Thông tin y tế Quốc gia về việc phê duyệt kế hoạch lựa chọn nhà thầu gói thầu “Nâng cấp Nền tảng Hỗ trợ tư vấn khám, chữa bệnh từ xa (Nền tảng VTelehealth)”


Trung tâm Thông tin y tế Quốc gia trân trọng đề nghị Quý Đơn vị có đủ năng lực tham gia chỉ định thầu rút gọn gói thầu trên và gửi hồ sơ cho Trung tâm.

Đầu mối liên hệ: Ông Mẫn Ngọc Anh, Trung tâm Thông tin y tế Quốc gia.
Điện thoại: 098.1995.198. Email: anhmn.cntt@moh.gov.vn.

Trân trọng cảm ơn!

Nơi nhận:

- Như trên;
- Giám đốc (để báo cáo);
- Các Phó Giám đốc (để biết);
- Lưu: VT, DVCĐS.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đinh Hải Long

PHỤ LỤC YÊU CẦU

(Kèm theo Công văn số 379/TTYQG-DVCĐS ngày 20 tháng 4 năm 2026
của Trung tâm Thông tin y tế Quốc gia)

1. Mục tiêu thực hiện:

Bổ sung tính năng thanh toán không dùng tiền mặt trên Nền tảng Hỗ trợ tư vấn khám, chữa bệnh từ xa phục vụ người dân và các cơ sở khám chữa bệnh, giúp tiết kiệm thời gian, công sức, tăng tính minh bạch trong thu phí, lệ phí và nghĩa vụ tài chính

2. Yêu cầu phạm vi

- Bổ sung tính năng thanh toán không tiền mặt sử dụng QRcode trên ứng dụng VTelehealth;

- Đảm bảo an toàn thông tin, bảo vệ dữ liệu cá nhân của người dân;

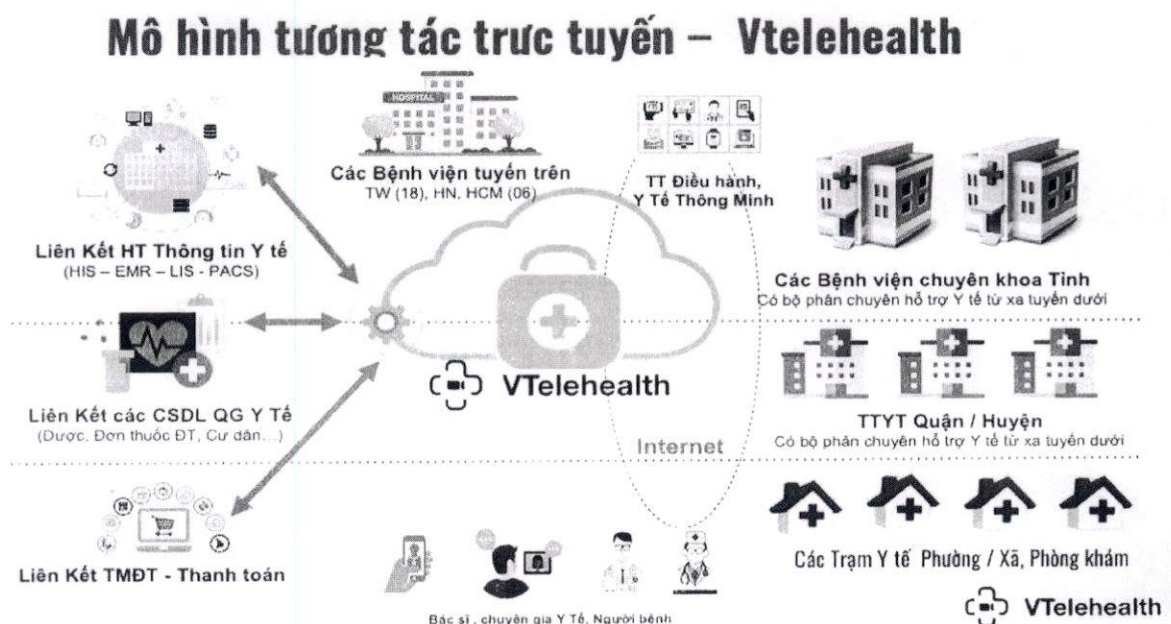
- Có tính năng tích hợp dữ liệu với Phần mềm quản lý bệnh viện hiện đang triển khai tại các cơ sở khám chữa bệnh;

- Có tính năng tích hợp dữ liệu với hệ thống ngân hàng

3. Hiện trạng Nền tảng Hỗ trợ tư vấn khám chữa bệnh từ xa (Nền tảng VTelehealth)

3.1. Mô hình triển khai hệ thống:

- Mô hình tổng quan của nền tảng:



Hình 1. Mô hình tương tác nền tảng VTelehealth

(Handwritten signature)

3.2. Mô tả các thành phần trong mô hình tổng thể:

- Hệ thống nền tảng VTelehealth gồm: hệ thống tương tác truyền hình trực tuyến, hệ thống lõi nền tảng, hệ thống nghiệp vụ nền tảng

- Các phần mềm ứng dụng giao diện đầu cuối phục vụ Cơ sở y tế, bác sĩ, người dân trên các môi trường và theo hoạt động khác nhau:

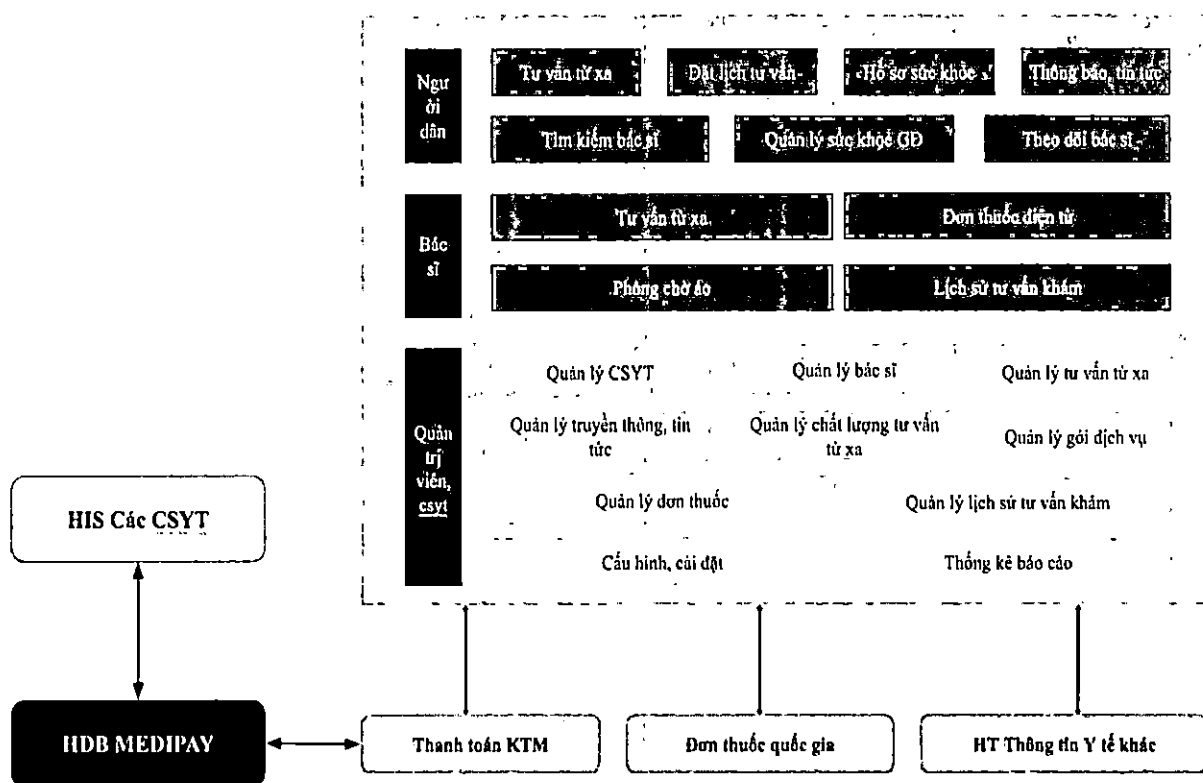
+ Dành cho cơ sở y tế sử dụng phiên bản trên môi trường web.

+ Ứng dụng di động cho Bác sĩ và người dân (bao gồm hệ điều hành IOS và Android).

- Các hệ thống thành phần gồm các giao diện lập trình tích hợp (API), phần mềm kết nối hệ thống thông tin y tế, cơ sở dữ liệu quốc gia lĩnh vực y tế, bảo hiểm và dân cư.

- Các hệ thống khác kết nối với nền tảng VTelehealth như: Hệ thống thông tin y tế của các Cơ sở y tế, Bộ y tế; Các CSDL ngành y tế; và các hệ thống dịch vụ gia tăng, tiện ích trong lĩnh vực y tế hoặc liên quan tới lĩnh vực y tế.

4. Mô hình triển khai hạ tầng cài đặt hệ thống

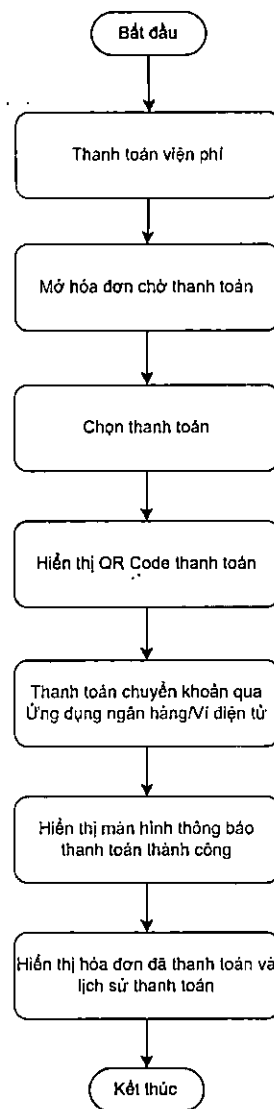


Hình 2: Mô hình triển khai hạ tầng cài đặt hệ thống

5. Các quy trình nghiệp vụ cần tin học hóa

- Nhóm chức năng mới liên quan đến thanh toán không tiền mặt:

5.1 Quy trình thanh toán viện phí



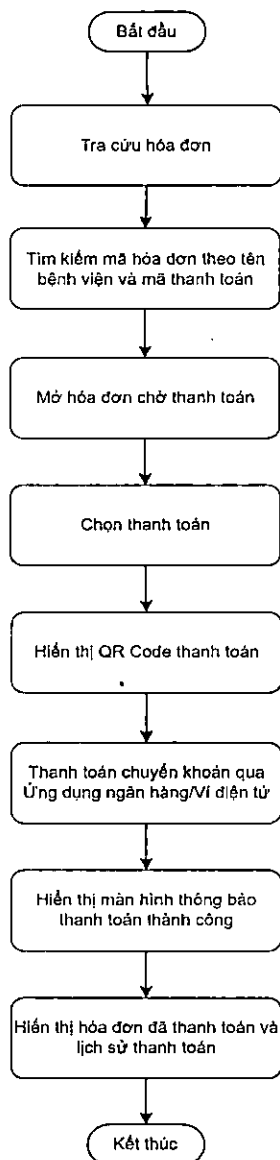
- Tác nhân: Người dân/Bệnh nhân

- Giải thích quy trình:

- + Người dân/Bệnh nhân chọn danh mục Thanh toán viện phí.
- + Người dân/Bệnh nhân mở hóa đơn chờ thanh toán.
- + Người dân/Bệnh nhân chọn thanh toán.
- + Ứng dụng hiển thị QR Code thanh toán theo hóa đơn.
- + Người dân/Bệnh nhân thực hiện tải mã QR Code
- + Người dân/Bệnh nhân sử dụng ứng dụng ngân hàng/Ví điện tử thanh toán quét mã QR Code vừa tải từ Nền tảng VTelehealth xuống. Ứng dụng hiển thị thông báo thanh toán thành công.
- + Ứng dụng hiển thị hóa đơn vừa thanh toán và xem lịch sử thanh toán.

5.2 Quy trình tra cứu hóa đơn thanh toán

anhmm.ttygg_Man Ngoc Anh_21/04/2026 15:49:20



- Tác nhân: Người dân/Bệnh nhân

- Giải thích quy trình:

- + Người dân/Bệnh nhân chọn danh mục Tra cứu hóa đơn.
- + Người dân/Bệnh nhân tìm kiếm mã hóa đơn theo tên bệnh viện và mã thanh toán.
- + Người dân/Bệnh nhân mở hóa đơn chờ thanh toán vừa tìm kiếm
- Người dân/Bệnh nhân chọn thanh toán.
- + Ứng dụng hiển thị QR Code thanh toán theo hóa đơn.
- + Người dân/Bệnh nhân sử dụng ứng dụng ngân hàng/Ví điện tử thanh toán quét mã QR Code vừa tải từ Nền tảng VTelehealth xuống. Ứng dụng hiển thị thông báo thanh toán thành công.

+ Ứng dụng hiển thị hóa đơn vừa thanh toán và xem lịch sử thanh toán.

6. Các tác nhân tham gia vào phần mềm

TT	Tên Actor	Mô tả tác nhân trong hệ thống	Phân loại tác nhân
1	Người dân/bệnh nhân	Người dân/bệnh nhân khám chữa bệnh từ xa và thanh toán không tiền mặt	Phức tạp
2	Quản trị hệ thống	Quản trị hệ thống quản trị người dùng	Phức tạp
3	Hệ thống khác	Liên thông kết nối	Đơn giản

7. Danh sách các chứng năng yêu cầu của phần mềm

1	Phân hệ Thanh toán viện phí
	Nhận thông báo thanh toán
	Danh sách hóa đơn chờ thanh toán
	Xem tin chi tiết hóa đơn gồm thông tin bệnh nhân và thông tin thanh toán
	Hiển thị QR Code thanh toán
	Tải mã QR Code
	Xem chi tiết thanh toán
	Tải biên lai
	Hiển thị thông tin hóa đơn và trạng thái thanh toán
	Hiển thị danh sách lịch sử thanh toán
	Lọc theo tháng, năm
	Ghi log giao dịch
	Xem chi tiết giao dịch
2	Phân hệ Tra cứu hóa đơn thanh toán
	Tra cứu hóa đơn theo bệnh viện hoặc phiếu
	Hướng dẫn tìm mã thanh toán
	Xem hóa đơn (thông tin chi tiết hóa đơn gồm thông tin bệnh nhân và thông tin thanh toán)

	Hiện thị QR Code thanh toán
	Tài mã QR Code
	Xem chi tiết thanh toán
	Tải biên lai
	Hiện thị thông tin hóa đơn và trạng thái thanh toán
	Hiện thị danh sách lịch sử thanh toán
	Lọc theo tháng, năm
	Ghi log giao dịch
	Xem chi tiết giao dịch
3	API liên thông tích hợp
	API truy vấn mã QR thanh toán
	API thông tin thanh toán
	API tra cứu kết quả thanh toán

8. Bảng sắp xếp thứ tự ưu tiên các yêu cầu chức năng của phần mềm

1	Thanh toán viện phí	
	Hệ thống gửi thông báo thanh toán	Dữ liệu đầu ra
	Người dân/Bệnh nhân quản lý danh sách hóa đơn chờ thanh toán	Dữ liệu đầu vào
	Người dân/Bệnh nhân xem tin chi tiết hóa đơn gồm thông tin bệnh nhân và thông tin thanh toán	Dữ liệu đầu ra
	Hệ thống Hiện thị QR Code thanh toán	Dữ liệu đầu ra
	Người dân/Bệnh nhân tải mã QR Code	Dữ liệu đầu ra
	Người dân/Bệnh nhân xem chi tiết thanh toán	Dữ liệu đầu vào
	Người dân/Bệnh nhân tải biên lai	Dữ liệu đầu vào
	Hệ thống hiển thị thông tin hóa đơn và trạng thái thanh toán	Dữ liệu đầu ra
	Hệ thống hiển thị danh sách lịch sử thanh toán	Dữ liệu đầu ra
	Hệ thống ghi log giao dịch	Dữ liệu đầu ra
	Quản trị hệ thống xem chi tiết giao dịch	Yêu cầu truy vấn

9. Bảng chuyển đổi yêu cầu chức năng sang trường hợp sử dụng

	Tên Use case	Tên tác nhân	Giao dịch (Transaction)	Phân loại theo BMT	Phân loại theo độ phức tạp
1	Thanh toán viện phí				
1.1	Quản lý hoá đơn	Người dân/bệnh nhân		B	Đơn giản
			Danh sách hoá đơn cần thanh toán		
			Tìm kiếm hoá đơn cần thanh toán		
			Xem chi tiết hoá đơn cần thanh toán		
1.2	Thanh toán	Người dân/bệnh nhân		B	Trung bình
			Hiển thị QR thanh toán		
			Tải mã QR thanh toán		
			Xem chi tiết thanh toán		
			Tải biên lai		
1.3	Lịch sử thanh toán	Người dân/bệnh nhân		B	Đơn giản
			Thông kê danh sách lịch sử thanh toán		

	Tên Use case	Tên tác nhân	Giao dịch (Transaction)	Phân loại theo BMT	Phân loại theo độ phức tạp
			Tìm kiếm lịch sử thanh toán theo thời gian		
			Xem chi tiết lịch sử thanh toán		
1.4	Thông báo	Người dân/bệnh nhân		B	Đơn giản
			Nhận thông báo thanh toán		
2	Tra cứu hoá đơn thanh toán	Người dân/bệnh nhân		B	Đơn giản
			Tìm kiếm mã hoá đơn theo: Tên bệnh viện, mã thanh toán		
			Xem hướng dẫn tra cứu		
			Xem chi tiết hoá đơn		
3	Báo cáo thống kê	Quản trị hệ thống	Thống kê theo ngày/tháng	B	Đơn giản
4	Quản lý log hệ thống	Quản trị hệ thống		B	Đơn giản
			Ghi log giao dịch		
			Xem chi tiết giao dịch		
5	Liên thông, tích hợp	Quản trị hệ thống		B	Đơn giản

	Tên Use case	Tên tác nhân	Giao dịch (Transaction)	Phân loại theo BMT	Phân loại theo độ phức tạp
			API truy vấn mã QR thanh toán		
			API thông tin thanh toán		
			API tra cứu kết quả thanh toán		

anhmn.tty@ig.Man Ngoc Anh 21/04/2026 14:20

10. Các yêu cầu phi chức năng

10.1 Yêu cầu cần đáp ứng đối với cơ sở dữ liệu

TT	Yêu cầu
1	Hệ thống chỉ cho phép người dùng đã qua xác thực được truy cập. Hệ thống sẽ cho phép tối thiểu ba loại người dùng được xác thực như người dùng nghiệp vụ, người dùng hệ thống nội bộ, và quản trị hệ thống.
2	Hệ thống sẽ thực thi các khái niệm về phiên của người sử dụng, đặc biệt là với đối tượng người dùng nghiệp vụ, trong đó các thông tin về hoạt động của người sử dụng từ lúc đăng nhập đến khi đăng xuất (tức là các phiên làm việc) được lưu lại trong cơ sở dữ liệu.
3	Hệ quản trị CSDL cho phép giám sát hoạt động lâu dài, sử dụng giao diện công cụ GUI để dễ dàng thao tác.
4	Hệ quản trị CSDL hỗ trợ việc sao chép và chia sẻ tải với một hệ thống khôi phục dự phòng.
5	Hệ quản trị CSDL sẽ cung cấp các công cụ tự động mở rộng để lưu trữ dữ liệu định kỳ.
6	Hệ quản trị CSDL sẽ cung cấp các công cụ tự động để định kỳ “làm sạch” dữ liệu nhằm đảm bảo sự nhất quán và toàn vẹn dữ liệu. Các công cụ phải lưu trữ các dữ liệu quá khứ để rollback nếu cần.
7	Cơ sở dữ liệu phải có khả năng lưu trữ với dung lượng lớn, trong thời gian lâu dài
8	Có khả năng lưu trữ được nhiều định dạng dữ liệu khác nhau như dữ liệu có cấu trúc, bán cấu trúc, phi cấu trúc dưới dạng tệp gắn kèm (dữ liệu tệp văn bản, dữ liệu phim, ảnh, âm thanh).

10.2 Yêu cầu cần đáp ứng đối với cơ sở dữ liệu

TT	Nội dung	Yêu cầu
1	Yêu cầu ATTT Cơ sở dữ liệu	
	ATTT Cơ sở dữ liệu	❖ Cài đặt Hệ quản trị CSDL an toàn.
		- Hệ quản trị CSDL phải được cài đặt trên máy chủ đảm bảo yêu cầu theo mục ATTT máy chủ.
		- Phiên bản Hệ quản trị CSDL phải được cập nhật tất cả bản vá security mới nhất.
		❖ Gỡ bỏ/tắt các thành phần thừa, thành phần không sử dụng.
		- Xóa các tài khoản, các CSDL thừa, không sử dụng.
		- Tắt các hàm tương tác với tài nguyên hệ điều hành (hàm đọc, ghi file, thực thi câu lệnh hệ thống).

TT	Nội dung	Yêu cầu
		<ul style="list-style-type: none"> ❖ Thiết lập chính sách tài khoản. - Các ứng dụng không dùng tài khoản có quyền quản trị để kết nối đến CSDL. - Tất cả các tài khoản phải có mật khẩu. - Các tài khoản phải được đặt mật khẩu theo quy định: <ul style="list-style-type: none"> + Mật khẩu có độ dài tối thiểu 8 ký tự + Mật khẩu bao gồm: ký tự chữ, số và ký tự đặc biệt + Thời gian bắt buộc phải thay đổi mật khẩu quản trị CSDL: tối đa là 03 tháng, mật khẩu mới không được trùng với 5 mật khẩu gần nhất. ❖ Phân quyền an toàn. - Không dùng các tài khoản quản trị, nhóm quản trị của hệ điều hành: root, Administrator, Local System... để chạy dịch vụ CSDL. - Phân quyền chỉ cho phép tài khoản chạy dịch vụ CSDL được phép truy cập (tất cả các hành động tương tác đến các thư mục chứa file dữ liệu, file log của CSDL). - Với mỗi ứng dụng, có một tài khoản kết nối CSDL riêng và chỉ cấp quyền tối thiểu đảm bảo hoạt động của ứng dụng. Tài khoản này và mật khẩu được mã hóa với 1 key bằng thuật toán bí mật (thư viện thuật toán này đã được build thành lib với cơ chế làm rối mã nguồn để chống dịch ngược thuật toán) và lưu trong file cấu hình. Chỉ ứng dụng mới có key và thuật toán giải mã, lấy ra thông tin tài khoản để truy cập Database. ❖ Cấu hình ghi log cho hệ quản trị CSDL. - Ghi log audit: cấu hình ghi log tất cả lần đăng nhập thành công và không thành công vào hệ quản trị CSDL.

TT	Nội dung	Yêu cầu
		<ul style="list-style-type: none"> - Log lưu trữ trong 3 tháng, các log quan trọng lưu trữ sau 3 tháng sẽ được đẩy sang hệ thống lưu trữ tập trung để lưu trữ tối thiểu 6 tháng. ❖ Cấu hình giới hạn truy cập. - Giới hạn chỉ được những IP cần thiết được kết nối đến CSDL ❖ Triển khai các giải pháp ngăn chặn việc truy suất trái phép dữ liệu của hệ thống: - Mã hóa dữ liệu (Data Encryption) bao gồm cả dữ liệu lưu trữ và dữ liệu trao đổi trên đường truyền - Phân loại và che giấu một phần hoặc toàn bộ dữ liệu nhạy cảm của hệ thống (Data Redaction and Masking sensitive Data) - Quản lý và ngăn chặn việc truy suất trái phép dữ liệu từ tất cả các tài khoản của người sử dụng đặc biệt là những tài khoản đặc quyền của hệ thống (Privileged User Controls). ❖ Triển khai các giải pháp kiểm soát truy cập tới cơ sở dữ liệu của bên thứ 3 độc lập với giải pháp sẵn có của hệ quản trị CSDL đảm bảo các yêu cầu sau: - Giám sát và quản lý mọi truy xuất đến Cơ sở dữ liệu và máy chủ CSDL (bao gồm cả truy xuất đến CSDL qua mạng và truy xuất trực tiếp trên máy chủ CSDL) tuân thủ theo các chính sách (policy/rule) an toàn thông tin cũng như các yêu cầu nghiệp vụ quy định (Activity Monitoring/Database Firewall) - Ghi nhận đầy đủ các thao tác của người sử dụng trên CSDL, có cơ chế cảnh báo thời gian thực và báo cáo định kỳ về tác động của người dùng lên hệ thống. (auditing and reporting)
2	Yêu cầu ATTT ứng dụng	
2.1	Quản lý xác thực	<ul style="list-style-type: none"> ❖ Tên đăng nhập phải là duy nhất, chỉ nên chứa tập các ký tự là chữ cái, chữ số, dấu gạch dưới.

TT	Nội dung	Yêu cầu
		<ul style="list-style-type: none"> ❖ Thiết lập mật khẩu người dùng ứng dụng tuân theo chính sách mật khẩu mạnh để tránh các tấn công dò, quét thông tin xác thực người dùng: <ul style="list-style-type: none"> - Mật khẩu có độ dài tối thiểu là 8 ký tự - Mật khẩu có chứa chữ cái, chữ số và kí tự đặc biệt ❖ 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. ❖ Đối với chức năng reset/ quên mật khẩu: <ul style="list-style-type: none"> - 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. - Nếu chức năng reset/quên mật khẩu thực hiện gửi mật khẩu qua email thì mật khẩu phải được sinh ngẫu nhiên và tuân theo chính sách mật khẩu mạnh. ❖ Mật khẩu người dùng được lưu trong cơ sở dữ liệu dưới dạng mã hash, không lưu thông tin mật khẩu dạng rõ. Khuyến nghị sử dụng thuật toán hash là SHA-256 hoặc SHA-512, thêm chuỗi salt vào mật khẩu trước khi thực hiện hash (salt là ngẫu nhiên và duy nhất với mỗi người dùng) ❖ Áp dụng cơ chế bảo vệ bằng Captcha hoặc các hình thức tương đương đối với chức năng Đăng nhập và các chức năng quan trọng khác của ứng dụng. Thực hiện kiểm tra tính hợp lệ của Captcha trước khi thực hiện chức năng chính của request. ❖ Chỉ sử dụng phương thức POST để submit các thông tin nhạy cảm (như thông tin định danh username/password), khuyến nghị sử dụng HTTPS để bảo vệ dữ liệu trên đường truyền.
2.2	Quản lý phiên đăng nhập	<ul style="list-style-type: none"> ❖ Session phải được thiết lập thời gian timeout, giá trị timeout cần cân bằng giữa nhu cầu thực hiện các

TT	Nội dung	Yêu cầu
		<p>chức năng của người dùng và yếu tố bảo mật.</p> <ul style="list-style-type: none"> ❖ Tạo mới session ngay sau khi đăng nhập thành công. Hủy session, xóa giá trị sessionId và các dữ liệu gắn với session đó khi người dùng đăng xuất. ❖ Áp dụng thuộc tính “HTTP-Only” cho các trường session cookie và thuộc tính “Secure” nếu ứng dụng sử dụng HTTPS. ❖ Đối với các chức năng quan trọng (các chức năng thêm, sửa, xóa CSDL,...), ứng với mỗi request cần thêm 1 token ngẫu nhiên và thực hiện kiểm tra tính hợp lệ của token này trước khi xử lý.
2.3	Phân quyền người dùng	<ul style="list-style-type: none"> ❖ Phía giao diện người dùng: Chỉ hiển thị các thành phần giao diện, đường dẫn, ... tương ứng với quyền của người dùng. Không sử dụng CSS, Javascript để ẩn hay vô hiệu hóa các giao diện, chức năng người dùng không được quyền truy cập. ❖ Phía server: <ul style="list-style-type: none"> - Kiểm tra quyền thực hiện chức năng (phân quyền chức năng) của người dùng trong mỗi request: kiểm tra người dùng hiện tại có được phép thực hiện chức năng hay không, đảm bảo người dùng không thể truy cập hay thực hiện các chức năng không được phép. Ví dụ người dùng bình thường không thể truy cập hay thực hiện các chức năng Quản lý hệ thống của đối tượng người dùng Quản trị viên - Kiểm tra quyền tác động tới miền dữ liệu (phân quyền dữ liệu) trong mỗi request - chức năng, đảm bảo không cho phép người dùng truy cập (xem, sửa, xóa,...) các dữ liệu không được phép. Ví dụ người dùng quản trị của đơn vị A không thể xem thông tin, sửa, xóa các cấu hình, thông tin người dùng,... của đơn vị B hay không thể thêm các dữ liệu vào đơn vị B.

anhmp.tyqg_Man Ngoc Anh_21/04/2026 15:49

TT	Nội dung	Yêu cầu
		<p>- Việc kiểm tra phân quyền phải dựa vào đối tượng được lưu tại server (ví dụ quyền người dùng lưu trong session trên server, hay trong CSDL), tránh trường hợp kiểm tra phân quyền người dùng bằng các giá trị gửi từ client (ví dụ gửi mã quyền - roleId hay quyền quản trị - isAdmin từ client và dùng các giá trị này để kiểm tra quyền).</p>
2.4	Kiểm soát dữ liệu đầu vào	<ul style="list-style-type: none"> ❖ Các xử lý validate dữ liệu phải thực hiện ở phía server, không sử dụng các ngôn ngữ phía client như Javascript để validate. ❖ Validate kiểu dữ liệu, phạm vi, độ dài dữ liệu và định dạng dữ liệu, nếu dữ liệu đầu vào bắt buộc là các ký tự đặc biệt, cần thiết lập danh sách whitelist các ký tự đầu vào mong muốn. ❖ Thực hiện html encode các ký tự đặc biệt (<, >, ', ", &, /) 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) để tránh mắc phải lỗ hổng bảo mật XSS, Html injection. ❖ Trường hợp dữ liệu được gửi từ client xuất hiện lại trong Response header cần lọc bỏ các ký tự đặc biệt \n, \r để tránh lỗ hổng HTTP Response splitting ❖ Tránh việc lưu trữ các dữ liệu nhạy cảm trên cookie, nếu cần lưu trữ thì phải thực hiện mã hóa các dữ liệu này với thuật toán đối xứng mạnh và key được lưu tại server. ❖ Hạn chế việc chuyển hướng, chuyển tiếp đến các URI khác. Nếu ứng dụng có chức năng này cần phải lập danh sách whitelist các URI được phép thực hiện chuyển hướng, chuyển tiếp. ❖ Thao tác với XML an toàn tránh các lỗ hổng về XML injection, XML external entity attack

TT	Nội dung	Yêu cầu
		<ul style="list-style-type: none"> ❖ Kiểm tra dữ liệu người dùng, encode các kí tự đặc biệt (<, >, /) khi tạo dữ liệu xml ❖ Tắt tính năng external entity resolve và remote doctype retrieval của xml parser khi đọc dữ liệu xml
2.5	Kiểm soát ngoại lệ và ghi log ứng dụng	<ul style="list-style-type: none"> ❖ Xử lý các ngoại lệ bằng try-catch và trả về các thông báo lỗi chung đã custom, thông báo lỗi trả về không được chứa các thông tin nhạy cảm của người dùng, hệ thống. Việc cấu hình error page có thể thực hiện trong web.config ❖ Các thông tin lỗi, ngoại lệ này phải được log lại để phục vụ bảo trì, xác định nguyên nhân lỗi ứng dụng. ❖ File log phải được đặt tại thư mục an toàn ngoài thư mục web. Không thực hiện ghi log các dữ liệu nhạy cảm (thông tin người dùng, sessionId,...).

10.3 Các yêu cầu cần đáp ứng về thời gian xử lý, độ phức tạp xử lý của các phần mềm

TT	Nhóm tiêu chí	Tiêu chí
1	Thời gian phản hồi trung bình	Hệ thống có thời gian phản hồi trung bình dưới 10 giây đối với mỗi luồng công việc chính riêng rẽ và không bao gồm các luồng mang tính chất thống kê, báo cáo (thời gian phản hồi được tính từ khi người sử dụng gửi yêu cầu đáp ứng tới hệ thống cho đến khi nhận được dữ liệu phản hồi từ hệ thống).
2	Thời gian phản hồi chậm nhất	Hệ thống có thời gian phản hồi chậm nhất dưới 30 giây đối với toàn bộ các thao tác trên toàn trang.
3	Hiệu suất làm việc của máy chủ dữ liệu	Hiệu suất làm việc trung bình của CPU trên máy chủ dữ liệu $\leq 75\%$.
4	Hiệu suất làm việc của máy chủ ứng dụng	Hiệu suất làm việc trung bình của CPU trên máy chủ ứng dụng $\leq 75\%$.
5	Truy cập đồng thời	Hệ thống có khả năng đáp ứng ít nhất 100 truy cập đồng thời

6	Số người sử dụng hoạt động đồng thời	Hệ thống có khả năng đáp ứng số người sử dụng hoạt động đồng thời (có thực hiện các tác vụ khác nhau phát sinh yêu cầu gửi đến hệ thống) ít nhất bằng 1/6 lần số lượng truy cập đồng thời (Mức độ hoạt động tương tự người sử dụng đã sử dụng thành thạo hệ thống).
---	--------------------------------------	---

10.4 Các yêu cầu về cài đặt, hạ tầng, đường truyền, an toàn vận hành, khai thác, sử dụng

- Hạ tầng phần cứng: Đảm bảo các yêu cầu về máy chủ, lưu trữ, và mạng, bao gồm các cấu hình tối thiểu về CPU, RAM, ổ đĩa cứng và băng thông mạng. Quan điểm sử dụng đối với hạ tầng phần cứng, theo hướng kế thừa các hạ tầng, tài nguyên hiện có của Chủ đầu tư, bao gồm tài nguyên vật lý và ảo hóa

- An toàn vận hành: Đảm bảo rằng hệ thống có cơ chế dự phòng (backup), khôi phục sau sự cố, và các biện pháp an toàn khi vận hành (hệ thống chống sập, bảo vệ dữ liệu).

- Đường truyền: Đảm bảo hệ thống có kết nối mạng ổn định, băng thông đủ lớn để phục vụ các tác vụ xử lý dữ liệu lớn và đồng thời.

- Cài đặt và bảo trì: Quá trình cài đặt và bảo trì hệ thống phải dễ dàng, cung cấp tài liệu và công cụ hỗ trợ kỹ thuật để người dùng hoặc quản trị viên có thể thực hiện nhanh chóng và chính xác

10.5 Các ràng buộc đối với hệ thống gồm: ràng buộc môi trường, sự phụ thuộc vào hệ thống nền tảng

- Ràng buộc môi trường: Hệ thống phải hoạt động tốt trong các điều kiện môi trường cụ thể như nhiệt độ, độ ẩm, và điều kiện vật lý của trung tâm dữ liệu.

- Sự phụ thuộc vào nền tảng: Hệ thống có thể phải phụ thuộc vào các công nghệ hoặc nền tảng cụ thể, như hệ điều hành (Windows, Linux....), cơ sở dữ liệu (Oracle, MySQL....), hoặc các công cụ lập trình (Java, .NET....)

10.6 Yêu cầu về phát triển phần mềm

Mobile App:

- Ngôn ngữ lập trình: Typescript
- Framework: React-native
- Hệ điều hành: Android/IOS

Web App:

- Ngôn ngữ lập trình: C#
- Framework
 - + Back-end: aspnetcore 8.0
 - + Front-end: angular 17.x

- Database: MariaDB, Redis
- Web Server: Kestrel, NGINX
- Hệ điều hành máy chủ: Ubuntu Linux LTS hoặc Rocky Linux 9

10.7 Yêu cầu về tính sẵn sàng với Ipv6

TT	Yêu cầu
1	Đảm bảo phần mềm hỗ trợ IPv6;
2	Đảm bảo đường truyền kết nối Internet cho Webserver hỗ trợ IPv6
3	Khai báo Webserver lắng nghe được các kết nối qua mạng IPv6
4	Khai báo bản ghi AAAA cho tên miền trên hệ thống DNS Hosting
5	Đảm bảo máy chủ DNS Hosting hỗ trợ IPv6
6	Sẵn sàng hỗ trợ địa chỉ Internet thế hệ mới IPv6, DNSSEC. Triển khai HTTPS sử dụng giao thức TLS v1.2 trở lên với các bộ mã hóa an toàn trong xác thực người dùng và truyền nhận các thông tin nhạy cảm (thông tin cá nhân, thông tin thanh toán).

10.8 Yêu cầu về mức độ chịu đựng sai hỏng đối với các lỗi cú pháp lập trình, lỗi logic trong xử lý dữ liệu, lỗi kiểm soát tính đúng đắn của dữ liệu đầu vào

TT	Yêu cầu
1	Các trường thông tin ngày tháng sẽ được lưu với 4 chữ số cho phần "Năm", và có thể được hiển thị theo tất cả các định dạng ngày chung dd/mm/yyyy.
2	Hệ thống phải hỗ trợ nhập, lưu trữ và hiển thị dữ liệu tiền tệ VND với ít nhất 15 chữ số nguyên và 2 số thập phân.
3	Hệ thống phải hỗ trợ kiểm tra tức thời tính hợp lệ của các giá trị nhập vào qua phương thức nhập trực tiếp.
4	Hệ thống phải hỗ trợ kiểm tra tức thời tính hợp lệ của các giá trị nhập vào qua phương thức nhập trực tiếp hoặc qua tệp dữ liệu.
5	Hệ thống phải cung cấp chức năng kiểm tra tính nhất quán và toàn vẹn của các trường dữ liệu có quan hệ ràng buộc với nhau trong cơ sở dữ liệu thông qua các quy tắc đã được định nghĩa như ràng buộc khóa khi xây dựng CSDL.
6	Các dữ liệu trước khi nhập vào hệ thống phải được kiểm tra tính đúng đắn về cấu trúc, định dạng và logic và phải thông báo ngay cho người sử dụng khi có lỗi xảy ra
7	Hệ thống phải hiển thị dấu thông báo rằng ô nhập là bắt buộc hoặc tùy chọn

TT	Yêu cầu
	nhập dữ liệu cho người dùng.
8	Hệ thống phải có các ô nhập dữ liệu với định dạng của dữ liệu nhập chuyên biệt ví dụ: Ô nhập ngày tháng, Ô nhập số...
9	Hệ thống có thứ tự các ô nhập tuân theo đúng logic của văn bản cần nhập, người dùng hoàn toàn có thể sử dụng bàn phím (không cần chuột) để di chuyển tới các ô nhập này.
10	Hệ thống phải hỗ trợ chế độ hiển thị danh sách để người dùng chọn đối với các ô nhập có dữ liệu cố định
11	Hệ thống phải có quy trình nhằm giảm thiểu các lỗi cú pháp lập trình, lỗi logic xử lý dữ liệu.
12	Các định dạng tập tin (tập tin nhập vào hệ thống, tập tin được xuất ra từ hệ thống, tập tin lưu trữ trong hồ sơ điện tử...) tuân thủ theo các định dạng tập tin (về văn bản, hình ảnh...) được quy định tại Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ trưởng Bộ Thông tin và Truyền thông.

10.9 Yêu cầu về mỹ thuật, kỹ thuật cần đạt được của các giao diện chương trình

TT	Yêu cầu
1	Hệ thống phải cung cấp giao diện trực quan, thân thiện với người sử dụng và phù hợp đối với các nhóm người sử dụng khác nhau.
2	Giao diện với người sử dụng đầu cuối dựa trên nền tảng web.
3	Đễ dàng tìm kiếm dịch vụ: người sử dụng dễ dàng tìm được dịch vụ sau tối đa 03 lần bấm chuột.
4	Giao diện ứng dụng phải thân thiện với người sử dụng và dễ dùng. Hỗ trợ tối đa sử dụng các chức năng bằng bàn phím máy tính. Các màn hình nhập và cập nhật dữ liệu về cơ bản phải thống nhất về các thao tác trên bàn phím cũng như về màu sắc, fonts chữ. Các màn hình tra cứu điều kiện lọc báo cáo cũng phải thống nhất với nhau. Các biểu tượng và phím nóng phải được thống nhất trong toàn bộ chương trình
5	Các giao diện phải được thiết kế đơn giản nhưng hiệu quả cao về thao tác, giảm thiểu việc mở quá nhiều tab, hiển thị và xử lý hình ảnh nhanh, màu sắc không gây cảm giác nhàm chán cho người sử dụng và theo một chuẩn giao diện thống nhất.
6	Hệ thống phải cho phép lưu trữ tất cả dữ liệu theo định dạng Unicode, chấp nhận tất cả các ký tự tiếng Việt có dấu.

TT	Yêu cầu
	Giao diện màn hình, các thông báo lỗi và trợ giúp là ngôn ngữ tiếng Việt theo chuẩn TCVN6909:2001 dựa trên bảng mã Unicode dựng sẵn (ISO 10646), với trợ giúp của các bộ gõ Unikey, Vietkey.
	Giao diện chương trình dùng các Font chuẩn của hệ thống như Arial hay Times News Romans. Người dùng không phải cài thêm bất cứ font chữ nào.
7	Các chức năng phần mềm được xây dựng với một cơ chế thông báo lỗi thân thiện và rõ ràng. Thông báo lỗi phải được Việt hóa tối đa, giúp cho người sử dụng biết được lý do gây ra lỗi để tránh lặp lại các trường hợp tương tự. Hệ thống báo lỗi xác định rõ ràng đâu là lỗi do người sử dụng gây ra và đâu là lỗi do hệ thống phần mềm gây ra và chỉ ra hướng khắc phục.
8	Với các lỗi do phần mềm/hệ thống gây ra, phải thông báo cho người dùng biết nguyên nhân và phương pháp xử lý. Có các biện pháp tự động phục hồi trong các trường hợp xác định. Tất cả các lỗi loại này phải được ghi lại thành log phục vụ cho mục đích bảo trì phần mềm, hệ thống.
9	Có tín hiệu thể hiện trạng thái hệ thống đang xử lý thông tin. Tín hiệu này phải được sử dụng thống nhất trong toàn bộ màn hình xử lý của Hệ thống (tín hiệu có thể là hình quay tròn, đồng hồ cát...).
10	Tuân thủ các quy định về chuẩn nội dung web theo Thông tư số 39/2017/TT-BTTTT ngày 15/12/2017 của Bộ trưởng Bộ Thông tin và Truyền thông.

10.10 Các yêu cầu về năng lực của cán bộ tham gia xây dựng, phát triển, nâng cấp, mở rộng phần mềm

Cán bộ tham gia thiết kế, xây dựng và phát triển phần mềm là kỹ sư CNTT có 2 năm kinh nghiệm lập trình ứng dụng web trở lên. Sử dụng thành thạo một trong các ngôn ngữ lập trình java, php, python, .NET hoặc tương đương.

10.11 Yêu cầu về sao lưu và khôi phục dữ liệu

Sao lưu hệ thống và dữ liệu:

Sử dụng giải pháp sao lưu sau: Sao lưu toàn bộ hệ thống sau khi cài đặt.

Thực hiện sao lưu hệ thống một lần ban đầu sau khi cài đặt và cấu hình các thành phần liên quan gồm: Hệ điều hành; Phần mềm ứng dụng; Các phần mềm hệ thống khác có liên quan.

Biện pháp này đảm bảo khi gặp sự cố sẽ phục hồi phần hệ thống mà không tốn thời gian cài đặt và cấu hình.

Sao lưu dữ liệu hàng ngày:

Dữ liệu sao lưu hàng ngày gồm toàn bộ CSDL của phần mềm tại đơn vị. Chế độ sao lưu dữ liệu là full backup (sao lưu toàn bộ dữ liệu) bằng cách sao lưu dữ liệu ra ổ cứng di động.

ll

Đặt chế độ tự động sao lưu vào một giờ cụ thể trong ngày (ví dụ 12h). Cán bộ quản trị thực hiện việc sao lưu dữ liệu ra ổ cứng dự phòng vào cuối giờ hàng ngày.

Khôi phục hệ thống và dữ liệu khi có sự cố:

Khôi phục hệ thống: Sử dụng các dữ liệu đã sao lưu toàn bộ hệ thống sau khi cài đặt, cấu hình chuẩn để khôi phục hệ thống. Thời gian khôi phục chỉ mất khoảng 01 tiếng.

Khôi phục dữ liệu: Sử dụng ổ cứng lưu trữ dữ liệu của ngày gần nhất để khôi phục lại CSDL của phần mềm.

Kiểm tra hoạt động của hệ thống sau khi khôi phục: Ước tính thời gian để khôi phục sự hoạt động của hệ thống trong trường hợp có sự cố với máy chủ (với giả thiết các hỏng hóc về phần cứng đã được khắc phục) là khoảng 02 giờ làm việc.

10.12 Các yêu cầu phi chức năng khác

- Yêu cầu đối với tài liệu hướng dẫn, trợ giúp: được xây dựng bản mềm và tích hợp vào menu phần mềm, bao gồm:

- + Tài liệu hướng dẫn người sử dụng.
- + Tài liệu hướng dẫn Quản trị hệ thống.
- + Tài liệu cài đặt và xử lý sự cố.
- + Kịch bản kiểm thử.
- Nhật ký thi công.
- Các tài liệu khác có liên quan

11. Kết quả thực hiện

1. Sản phẩm bàn giao: Tính năng thanh toán không tiền mặt được tích hợp trên Nền tảng Hỗ trợ tư vấn khám, chữa bệnh từ xa.

2. Hồ sơ, tài liệu bao gồm:

- + Biên bản nghiệm thu và bàn giao sản phẩm.
- + Bộ cài đặt và mã nguồn của phần mềm.
- + Tài liệu thiết kế phần mềm.
- + Tài liệu hướng dẫn sử dụng và quản trị hệ thống.
- + Tài liệu hướng dẫn cài đặt.
- + Tài liệu API liên thông, tích hợp

(Các sản phẩm được ghi vào đĩa 02 đĩa CD hoặc thiết bị lưu trữ)