CỤC HÀNG HẢI VÀ ĐƯỜNG THỦY VIỆT NAM
CẢNG VỤ HÀNG HẢI THỪA THIÊN HUẾ

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

Số: 261/QĐ-CVHHTTH

Huế, ngày 20 tháng 11 năm 2025

QUYẾT ĐỊNH
Về việc phê duyệt cấp độ an toàn hệ thống thông tin Cảng vụ Hàng hải Thừa Thiên Huế

GIÁM ĐỐC CẢNG VỤ HÀNG HẢI THỪA THIÊN HUẾ

Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015;

Căn cứ Luật An ninh mạng số 24/2018/QH14 ngày 12/6/2018;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 1343/QĐ-BXD ngày 15/8/2025 của Bộ trưởng Bộ Xây dựng về việc tổ chức lại Cảng vụ Hàng hải Thừa Thiên Huế trực thuộc Cục Hàng hải và Đường thủy Việt Nam;

Xét đề nghị của Trưởng phòng Tổ chức Hành chính.

QUYẾT ĐỊNH

Điều 1. Phê duyệt cấp độ an toàn hệ thống thông tin đối với hệ thống thông tin Cảng vụ Hàng hải Thừa Thiên Huế cụ thể như sau:

1. Thông tin chung

a) Tên hệ thống thông tin: Hệ thống thông tin Cảng vụ Hàng hải Thừa Thiên Huế

b) Đơn vị vận hành hệ thống thông tin: Cảng vụ Hàng hải Thừa Thiên Huế

c) Địa chỉ: Số 06 Nguyễn Văn Tuyết, phường Thuận An, thành phố Huế

2. Cấp độ an toàn hệ thống thông tin: Cấp độ 1

3. Phương án bảo đảm an toàn thông tin:

Phương án bảo đảm an toàn thông tin trong quá trình vận hành hệ thống tương ứng với cấp độ 1 là phù hợp với quy định tại Nghị định số 85/2016/NĐ-CP

ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

(Có Hồ sơ cấp độ 1 an toàn hệ thống thông tin Cảng vụ Hàng hải Thừa Thiên Huế kèm theo)

Điều 2. Tổ chức thực hiện

1. Phòng Tổ chức Hành chính có trách nhiệm:

- Tổ chức quản lý, vận hành, bảo đảm an toàn hệ thống thông tin Cảng vụ Hàng hải Thừa Thiên Huế tương ứng với cấp độ 1 theo hồ sơ đề xuất và quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

- Theo dõi, đôn đốc công chức, viên chức, người lao động đơn vị thực hiện theo các quy định nêu trên;

- Kiểm tra, giám sát việc thực hiện Quyết định này, báo cáo Giám đốc Cảng vụ Hàng hải Thừa Thiên Huế theo quy định.

2. Các phòng, đơn vị trực thuộc có trách nhiệm:

- Thực hiện nghiêm các phương án bảo đảm an toàn thông tin tương ứng với Cấp độ 1 theo hồ sơ đề xuất và quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông.

Điều 3. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 4. Trưởng các phòng, đơn vị trực thuộc Cảng vụ Hàng hải Thừa Thiên Huế chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 4;
- Phó Giám đốc;
- Lưu: VT, TCHC.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
CẢNG VỤ HÀNG HẢI THỪA THIÊN HUẾ
CỤC HÀNG HẢI VÀ ĐƯỜNG THỦY VIỆT NAM

Đinh Quang Đăng

CỤC HÀNG HẢI VÀ ĐƯỜNG THỦY VIỆT NAM

CẢNG VỤ HÀNG HẢI THỪA THIÊN HUẾ

HỒ SƠ CẤP ĐỘ 1
HỆ THỐNG THÔNG TIN
CỦA CẢNG VỤ HÀNG HẢI THỪA THIÊN HUẾ

(Ban hành kèm theo Quyết định số 26 /QĐ-CVHHTTH ngày 20/11/2025 của Giám đốc Cảng vụ Hàng hải Thừa Thiên Huế)

Huế - 2025

MỤC LỤC

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
1.	CNTT	Công nghệ thông tin
2.	CSDL	Cơ sở dữ liệu
3.	LAN	Mạng nội bộ
4.	VPN	Virtual Private Network
5.	DNS	Domain Name Server

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

1. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: Cảng vụ Hàng hải Thừa Thiên Huế

- Quy định chức năng, nhiệm vụ và quyền hạn: Thông tư số 18/TT-BXD ngày 30/6/2025 của Bộ trưởng Bộ Xây dựng quy định về tổ chức và hoạt động của Cảng vụ hàng hải, Cảng vụ đường thủy nội địa

Người đại diện: Đinh Quang Đăng, Chức vụ: Giám đốc

Địa chỉ: Số 06 Nguyễn Văn Tuyết, phường Thuận An, thành phố Huế

Thông tin liên hệ:

- Số điện thoại: 0234.3866156 - Fax: 0234.3866240

- Thư điện tử: cangvu.hue@vinamarine.gov.vn

2. Thông tin Đơn vị vận hành

- Tên Đơn vị vận hành: Cảng vụ Hàng hải Thừa Thiên Huế

- Quy định chức năng, nhiệm vụ và quyền hạn: Thông tư số 18/TT-BXD ngày 30/6/2025 của Bộ trưởng Bộ Xây dựng quy định về tổ chức và hoạt động của Cảng vụ hàng hải, Cảng vụ đường thủy nội địa

Người đại diện: Đinh Quang Đăng, Chức vụ: Giám đốc

Địa chỉ: Số 06 Nguyễn Văn Tuyết, phường Thuận An, thành phố Huế

Thông tin liên hệ:

- Số điện thoại: 0234.3866156 - Fax: 0234.3866240

- Thư điện tử: cangvu.hue@vinamarine.gov.vn

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống Mạng LAN: Hệ thống thông tin của Cảng vụ Hàng hải Thừa Thiên Huế được thiết lập để phục vụ công tác chỉ đạo điều hành và cung cấp dịch vụ trong phạm vi Cảng vụ Hàng hải Thừa Thiên Huế

- Đối tượng phục vụ của hệ thống:

+ Dùng cho công chức, viên chức, người lao động Cảng vụ Hàng hải Thừa Thiên Huế

+ Dùng cho tổ chức, cá nhân đến liên hệ công tác tại đơn vị.

- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi trung tâm tích hợp dữ liệu:

+ Hệ thống Mạng LAN.

Ngoài hệ thống mạng LAN trên, hiện nay đơn vị đang sử dụng thêm một số hệ thống thông tin khác:

+ Hệ thống Quản lý Văn bản (V-Office).

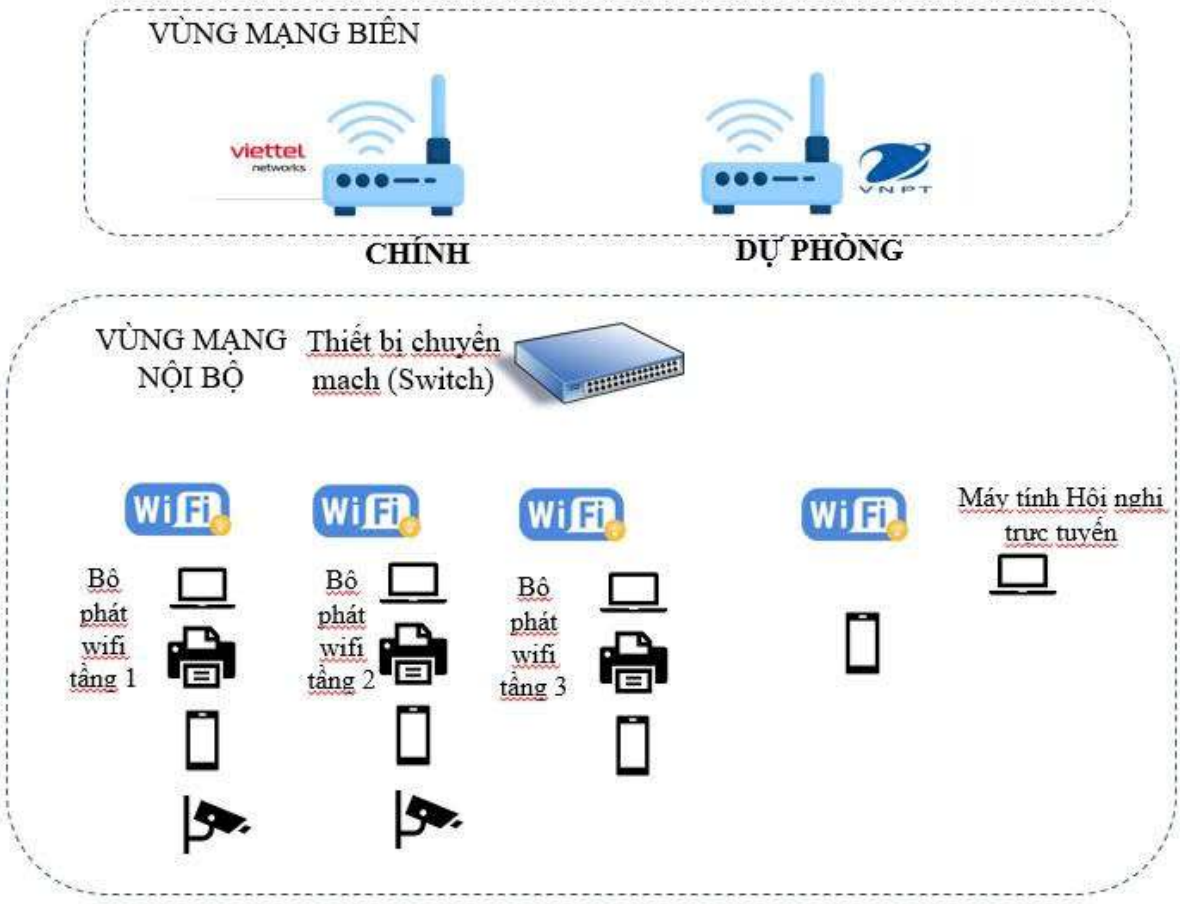
+ Hệ thống Trang thông tin điện tử (Website đơn vị).

+ Phần mềm thủ tục điện tử tàu biển vào, rời cảng.

+ Hệ thống cơ sở dữ liệu khác: Phần mềm phổ cập, kế toán Misa, …

4. Mô tả cấu trúc của hệ thống

4.1. Mô hình logic tổng thể



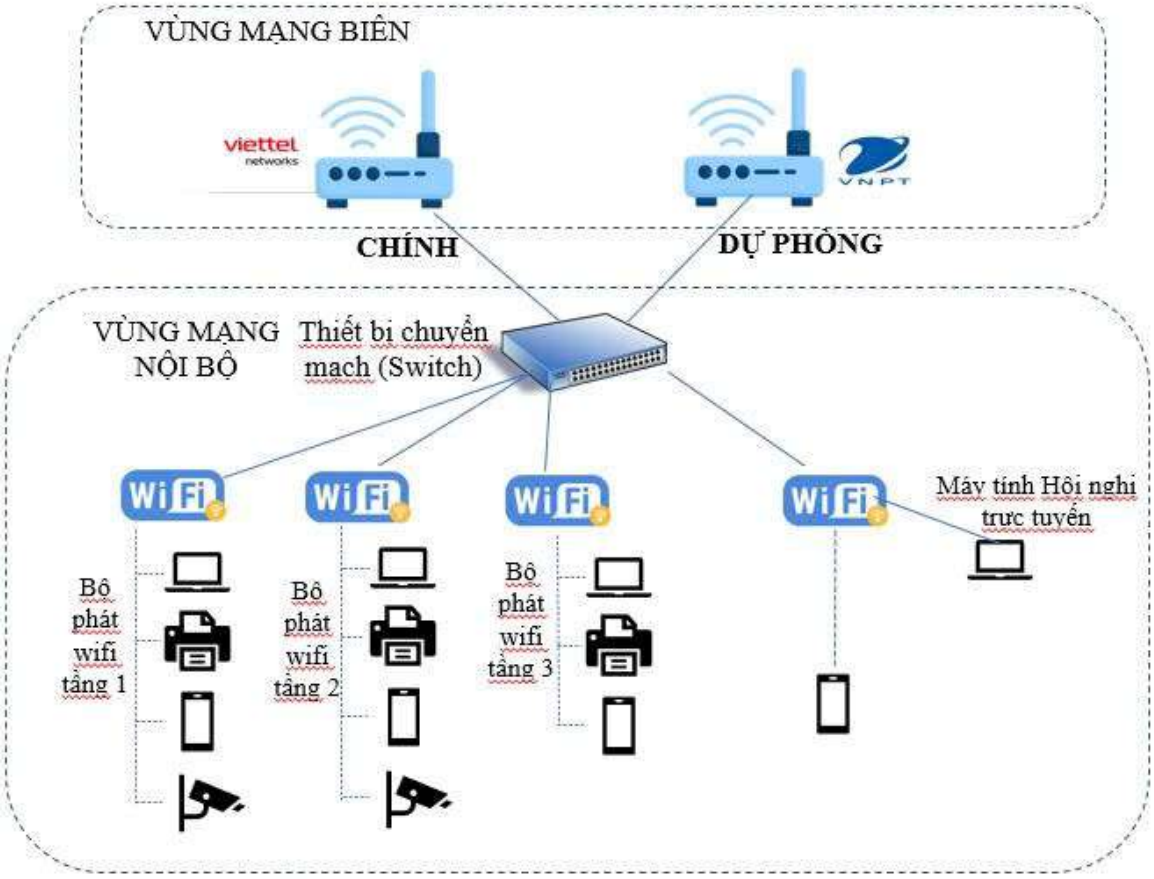
Hình 1. Cấu trúc logic của hệ thống

Các vùng mạng được thiết kế như sau:

+ Vùng mạng biên được thiết kế để kết nối hệ thống ra các mạng bên ngoài và mạng Internet.

+ Vùng mạng nội bộ đặt các thiết bị nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống.

4.2. Mô hình kết nối vật lý



Hình 2. Kết nối vật lý của hệ thống

4.3. Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Modem/VIETTEL (MẠNG CHÍNH)	Vùng mạng biên	Kết nối và định tuyến động với các Router của ISP.
	Modem/VNPT (DỰ PHÒNG)		
2	Firewall/DrayTek Vigor2925	Vùng mạng biên	Thiết bị tường lửa được thiết lập để quản lý, kiểm soát truy cập vào/ra giữa hệ thống với

			vùng mạng nội bộ, vùng mạng biên.
3	Switch LGS108/LINKSYS	Vùng mạng nội bộ	Chuyển mạch trung tâm đảm bảo tốc độ vận chuyển và liên kết với các lớp mạng
4	Wifi/DRAYTEK; UNIFI	Vùng mạng nội bộ	Thiết bị cung cấp kết nối internet không dây cho vùng mạng nội bộ

Bảng 1. Danh mục thiết bị sử dụng trong hệ thống

4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

STT	Tên dịch vụ	Máy chủ/Ứng dụng cài đặt/Vùng mạng/HĐH	Mục đích sử dụng
1	Phần mềm thủ tục điện tử tàu biển vào rời cảng	Server01/Cài đặt Web-App/Vùng DMZ/HĐH CentOS 7	Phục vụ cho công chức thủ tục tàu thuyền xử lý thủ tục hành chính tàu biển vào rời cảng biển liên thông với Cổng thông tin một cửa quốc gia.

Bảng 2. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

STT	Vùng mạng	IP Private	IP Public
1	Vùng mạng nội bộ	192.168.1.1/140	117.2.126.131

Bảng 3. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

1. Danh mục hệ thống thông tin và cấp độ đề xuất

Hệ thống thông tin của Cảng vụ Hàng hải Thừa Thiên Huế bao gồm hệ thống thành phần với cấp độ đề xuất tương ứng, bao gồm:

STT	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống Mạng LAN	1	Điều 7/NĐ85

2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin

Hệ thống Mạng LAN chỉ xử lý thông tin công khai và phục vụ hoạt động nội bộ cho công chức, viên chức, người lao động của Cảng vụ Hàng hải Thừa Thiên Huế. Căn cứ theo quy định tại Điều 7/NĐ85, hệ thống này được đề xuất cấp độ 1.

PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

Thuyết minh phương án về quản lý bao gồm các nội dung sau:

1. Thiết lập chính sách an toàn thông tin

2. Tổ chức bảo đảm an toàn thông tin

3. Bảo đảm nguồn nhân lực

4. Quản lý thiết kế, xây dựng hệ thống

5. Quản lý vận hành hệ thống

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

Đối với những yêu cầu quản lý chưa đáp ứng các yêu cầu an toàn trong Thuyết minh này, Đơn vị vận hành sẽ cập nhật, bổ sung trình Chủ quản hệ thống thông tin ban hành trong vòng 06 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Thuyết minh phương án về kỹ thuật bao gồm các nội dung:

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

1.2. Kiểm soát truy cập từ bên ngoài mạng

1.3. Nhật ký hệ thống

1.4. Phòng chống xâm nhập

1.5. Bảo vệ thiết bị hệ thống

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

2.2. Kiểm soát truy cập

2.3. Nhật ký hệ thống

2.4. Phòng chống xâm nhập

2.5. Phòng chống phần mềm độc hại

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

3.2. Kiểm soát truy cập

3.3. Nhật ký hệ thống

4. Bảo đảm an toàn dữ liệu

4.1. Sao lưu dự phòng

Đối với các yêu cầu kỹ thuật chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, Đơn vị vận hành sẽ triển khai nâng cấp, thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong vòng 18 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống của Cảng vụ Hàng hải Thừa Thiên Huế sẽ bao gồm các thuyết minh thành phần sau:

STT	Hệ thống	Cấp độ đề xuất	Nội dung thuyết minh
1	Thuyết minh phương án đáp ứng yêu cầu quản lý	1	Phụ lục I
2	Thuyết minh phương án đáp ứng yêu cầu kỹ thuật đối với Hệ thống Mạng LAN	1	Phụ lục II

PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 1

5.1.1. Thiết lập chính sách an toàn thông tin

5.1.1.1. Chính sách an toàn thông tin

Yêu cầu	Xây dựng chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống nhằm bảo đảm tính sẵn sàng của hệ thống trong quá trình vận hành, khai thác.
Hiện trạng	Đáp ứng *(Tham chiếu Điều 5, Điều 6 Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	1. Quản lý an toàn mạng: a) Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật. b) Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa tích hợp tường lửa trên router và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng. c) Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn. 2. Quản lý an toàn máy chủ và ứng dụng: a) Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phương án giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị. b) Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường (Ví

	dụ: user không có quyền nhưng cố tình truy xuất đến các file lưu mật khẩu…). 3. Quản lý an toàn dữ liệu: a) Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu. b) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành. c) Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên. 4. Quản lý an toàn người sử dụng đầu cuối: a) Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu. b) Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích kinh doanh của công ty. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu. c) Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP). Cần sử dụng cơ chế xác thực và sử dụng giao thức mạng an toàn d) Đơn vị chuyên trách về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa. e) Đơn vị chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc. f) Đơn vị chuyên trách về an toàn thông tin thường xuyên theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

5.1.1.2. Xây dựng và công bố

Yêu cầu	Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng.
Hiện trạng	Đáp ứng *(tham chiếu Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng Xây dựng và công bố Quy chế bảo đảm an toàn thông tin: 1. Quy chế được lấy ý kiến cấp có thẩm quyền, đơn vị liên quan trước khi công bố áp dụng 2. Quy chế được Giám đốc Cảng vụ Hàng hải Thừa Thiên Huế ban hành.

5.1.1.3. Rà soát, sửa đổi

Yêu cầu	Chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.
Hiện trạng	Đáp ứng. Tham chiếu Điều 11 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế) ngày 30/10/2025*
Phương án	Rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin: Trong quá trình thực hiện, nếu có vướng mắc, các tổ chuyên môn, cá nhân phản ánh về Ban Lãnh đạo (qua phòng Tổ chức Hành chính) để xem xét, sửa đổi, bổ sung cho phù hợp thực tiễn./.

5.1.2. Tổ chức bảo đảm an toàn thông tin

5.1.2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Có cán bộ có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin
Hiện trạng	Đáp ứng. Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	1. Phòng Tổ chức Hành chính chịu trách nhiệm quản lý, bảo trì, cập nhật hệ thống phần mềm, thiết bị mạng, sao lưu dữ liệu. 2. Bố trí cán bộ có trình độ về công nghệ thông tin thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa; theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

5.1.2.2. Phối hợp với những cơ quan/tổ chức có thẩm quyền

Yêu cầu 5.1.2.2.a	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin;
Hiện trạng	Đáp ứng Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Phòng Tổ chức Hành chính chủ trì, phối hợp với Công an thành phố Huế và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hoặc theo chỉ đạo của Lãnh đạo đơn vị.
Yêu cầu 5.1.2.2.b	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.

Hiện trạng	Đáp ứng. Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Phòng Tổ chức Hành chính phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin hoặc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng

5.1.3. Bảo đảm nguồn nhân lực

5.1.3.1. Tuyển dụng

Yêu cầu	Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng.
Hiện trạng	Đáp ứng. Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Phòng Tổ chức Hành chính tham mưu công tác tuyển dụng vị trí làm về an toàn thông tin có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng.

5.1.3.2. Trong quá trình làm việc

Yêu cầu 5.1.3.2.a	Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống
Hiện trạng	Đáp ứng. Tham chiếu *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế*

Phương án	Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc: Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống a) Với người sử dụng: - Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT. - Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT. - Cá nhân, tổ chức phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị. b) Với cán bộ quản lý và vận hành hệ thống - Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin. - Cán bộ chuyên trách phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.
Yêu cầu 5.1.3.2.b	Có hình thức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.
Hiện trạng	Đáp ứng. Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Tuyên truyền, hướng dẫn, hỗ trợ các phòng, đơn vị trực thuộc trong việc sử dụng an toàn hệ thống CNTT.

5.1.3.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu	Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.
Hiện trạng	Đáp ứng. Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Thực hiện cấp, thay đổi, thu hồi quyền truy cập các phần mềm quản lý, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của đơn vị trong trường hợp giao bố trí, thay đổi nhân sự hoặc nghỉ việc.

5.1.4. Quản lý thiết kế, xây dựng hệ thống thông tin

5.1.4.1. Thiết kế an toàn hệ thống thông tin

Yêu cầu 5.1.4.1.a	Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.
Hiện trạng	Đáp ứng. Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.
Yêu cầu 5.1.4.1.b	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.
Hiện trạng	Đáp ứng. Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số*

	253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)
Phương án	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

5.1.4.2. Thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.
Hiện trạng	Đáp ứng. Hệ thống thông tin hiện tại của đơn vị đã được đưa vào sử dụng, hoạt động ổn định.
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: 1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống, trình cấp có thẩm quyền phê duyệt, trước khi thực hiện thử nghiệm và nghiệm thu hệ thống. 2. Hệ thống phải được thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng theo nội dung, kế hoạch được phê duyệt.

5.1.5. Quản lý vận hành hệ thống thông tin

5.1.5.1. Quản lý an toàn mạng

Yêu cầu	Xây dựng và thực thi chính sách, quy trình quản lý vận hành hoạt động bình thường của hạ tầng mạng.
Hiện trạng	Đáp ứng. Tham chiếu Điều 5 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Quy định về quản lý an toàn mạng: 1. Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định

	danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật. 2. Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.

5.1.5.2. Quản lý an toàn máy chủ và ứng dụng

Yêu cầu	Xây dựng và thực thi chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.
Hiện trạng	Đáp ứng. Tham chiếu Điều 6 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Quy định về quản lý an toàn máy chủ và ứng dụng: 1. Quy định với máy chủ a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo hoạt động liên tục. b) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho hệ thống máy chủ. c) Máy chủ phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Thực hiện biện pháp phòng chống xâm nhập; Phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao. d) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. đ) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt.

	e) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế. g) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. 2. Quy định với ứng dụng: a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật. b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn. c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng. d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị.

5.1.5.3. Quản lý an toàn dữ liệu

Yêu cầu	Có phương án sao lưu dự phòng thông tin, dữ liệu, cấu hình hệ thống.
Hiện trạng	Đáp ứng. Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Quy định về quản lý an toàn dữ liệu: 1. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

	2. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. 3. Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống. 4. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ 5. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền. 6. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

5.1.6. Phương án Quản lý rủi ro an toàn thông tin

Yêu cầu	Có chính sách, quy trình quản lý rủi ro an toàn thông tin
Hiện trạng	Đáp ứng. Tham chiếu *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Phương án quản lý rủi ro an toàn thông tin phải được xây dựng trong Quy chế bảo đảm an toàn, trong đó cần làm rõ các nội dung sau đây: 1. Xác định mức rủi ro. 2. Quy trình đánh giá và quản lý rủi ro. 3. Biện pháp kiểm soát rủi ro.

5.1.7. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

Yêu cầu	Có quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ
Hiện trạng	Đáp ứng. Tham chiếu Điều 10 *Quy chế bảo đảm an toàn thông tin, an ninh mạng Cảng vụ Hàng hải Thừa Thiên Huế theo Quyết định số 253/QĐ-CVHHTTH ngày 30/10/2025 của Cảng vụ Hàng hải Thừa Thiên Huế)*
Phương án	Thực hiện cấp, thay đổi, thu hồi quyền truy cập các phần mềm quản lý, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của đơn vị trong trường hợp giao bố trí, thay đổi nhân sự hoặc nghỉ việc.

PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG CẤP ĐỘ 1

Hệ thống chỉ xử lý thông tin nội bộ và xử lý thông tin công khai, phục vụ hoạt động nội bộ cho cán bộ của *Cảng vụ Hàng hải Thừa Thiên Huế*. Căn cứ theo quy định tại Điều 7/NĐ85, hệ thống này được đề xuất cấp độ 1

Phương án bảo đảm an toàn thông tin cấp độ 1 được thuyết minh như dưới đây:

5.2.1. Bảo đảm an toàn mạng

5.2.1.1. Thiết kế hệ thống

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, bao gồm các vùng mạng:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng nội bộ	Có	Cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối, các thiết bị khác của người sử dụng vào hệ thống
2	Vùng mạng biên	Có	Cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác

b) Phương án thiết kế bảo đảm các yêu cầu:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có	Các thiết bị hệ thống/máy chủ được thiết lập cấu hình cho phép quản trị từ xa an toàn. Sử dụng tường lửa tích hợp Router modem
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Có	Truy cập giữa các vùng mạng được quản lý và phòng chống xâm nhập sử dụng Modem Wifi được bảo mật bằng mật khẩu.
3	Phương án phòng chống mã độc cho		Sử dụng sản phẩm Antivirus Kaspersky hoặc BKAV. Sử dụng Phần mềm bản quyền bảo mật website (Bản quyền phần

	máy chủ và máy trạm		mềm chứng chỉ số SSL) cho Website đơn vị quản lý

5.2.1.2. Kiểm soát truy cập từ bên ngoài mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet	Có	Hệ thống được thiết lập chỉ cho phép kết nối mạng có hỗ trợ mã hóa, xác thực khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet thông qua Modem
2	Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài	Có	Hệ thống được thiết lập chỉ cho phép kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể thông qua Modem

5.2.1.3. Nhật ký hệ thống

Yêu cầu	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị mạng chính
Thiết bị	
Modem/VIETTEL Modem/VNPT	+
Firewall (tích hợp router DrayTek Vigor 2925)	+
Switch LGS108/LINKSYS	+

Wifi/DRAYTEK; UNIFI	+

5.2.1.4. Phòng chống xâm nhập

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống xâm nhập để bảo vệ vùng DMZ	Có	Các vùng mạng được triển khai hệ thống IPS, hoạt động ở chế độ Inline cho phép phát hiện và phòng chống xâm nhập.
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng	Có	Đã thiết lập chức năng tự động cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng đều được thiết lập trên các thiết bị IPS.

5.2.1.5. Bảo vệ thiết bị hệ thống

Yêu cầu **Thiết bị**	Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa;	Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (Nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa.
Modem/VIETTEL Modem/VNPT	+	+
Firewall (tích hợp router DrayTek Vigor 2925)	+	+
Switch LGS108/LINKSYS	+	+
Wifi/DRAYTEK; UNIFI	+	+

5.2.2. Bảo đảm an toàn máy chủ

5.2.2.1. Xác thực

Yêu cầu	Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ;	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng
Máy chủ			
Server01/Cài đặt Web-App /Vùng DMZ/HĐH CentOS 7	+	+	+

5.2.2.2. Kiểm soát truy cập

Yêu cầu	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa
Máy chủ	
Server01/Cài đặt Web-App /Vùng DMZ/HĐH CentOS 7	+

5.2.2.3. Nhật ký hệ thống

Yêu cầu	Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ	Đồng bộ thời gian giữa máy chủ với máy chủ thời gian
Máy chủ		
Server01/Cài đặt Web-App	+	+

/Vùng DMZ/HĐH CentOS 7		

5.2.2.4. Phòng chống xâm nhập

Yêu cầu	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ
Máy chủ		
Server01/Cài đặt Web-App /Vùng DMZ/HĐH CentOS 7	+	+

5.2.2.5. Phòng chống phần mềm độc hại

Yêu cầu	Sử dụng sản phẩm Antivirus Kaspersky hoặc BKAV. Sử dụng Phần mềm bản quyền bảo mật website (Bản quyền phần mềm chứng chỉ số SSL) cho Website đơn vị quản lý
Máy chủ	
Server01/Cài đặt Web-App/Vùng DMZ/HĐH CentOS 7	+

5.2.3. Bảo đảm an toàn ứng dụng

5.2.3.1. Xác thực

Yêu cầu	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng
Ứng dụng			

Cổng thông tin nội bộ	+	+	+

5.2.3.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng
Ứng dụng		
Cổng thông tin nội bộ	+	+

5.2.3.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng.
Ứng dụng	
Cổng thông tin nội bộ	+

5.2.4. Bảo đảm an toàn dữ liệu

5.2.4.1. Sao lưu dự phòng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu quan trọng trên hệ thống.	Có	Thông tin, dữ liệu quan trọng trên hệ thống đảm bảo được sao lưu dự phòng như: tập tin cấu hình hệ thống, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ