ỦY BAN NHÂN DÂN HUYỆN CẨM XUYÊN

TRUNG TÂM Y TẾ

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 1
HỆ THỐNG CỔNG THÔNG TIN: CỔNG THÔNG TIN ĐIỆN TỬ TRUNG TÂM Y TẾ HUYỆN CẨM XUYÊN

Tỉnh Hà Tĩnh – 2024

MỤC LỤC

5.1.1. Thiết lập chính sách an toàn thông tin

5.1.2. Tổ chức bảo đảm an toàn thông tin

5.1.3. Bảo đảm nguồn nhân lực

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

5.1.5. Quản lý vận hành hệ thống thông tin

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

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

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

5.2.1. Bảo đảm an toàn mạng

5.2.2. Bảo đảm an toàn máy chủ

5.2.3. Bảo đảm an toàn ứng dụng

5.2.4. Bảo đảm an toàn dữ liệu

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	Vitural 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: UBND huyện Cẩm xuyên

- Quy định chức năng, nhiệm vụ và quyền hạn: Căn cứ theo Luật Tổ chức Chính quyền địa phương ngày 19/6/2015;Luật sửa đổi, bổ sung một số điều của Luật tổ chức Chính phủ và Luật tổ chức Chính quyền địa phương ngày 22/11/2019

- Người đại diện: Hà Văn Bình Chức vụ: Chủ tịch UBND huyện.

- Địa chỉ: Thị trấn Cẩm Xuyên - Tỉnh Hà Tĩnh

- Thông tin liên hệ:

+ Số điện thoại: 0912485388

+ Thư điện tử: havanbinh.cx@hatinh.gov.vn

2. Thông tin Đơn vị vận hành

- Tên tổ chức: Trung tâm y tế

- Quy định chức năng, nhiệm vụ và quyền hạn: Thông tư số 07/2021/TT-BYT ngày 27/5/2021 của Bộ Y tế hướng dẫn chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm y tế huyện, quận, thị xã, thành phố thuộc tỉnh, thành phố thuộc thành phố trực thuộc Trung ương; Quyết định số 634/QĐ - UBND ngày 11/3/2024 của UBND tỉnh Hà Tĩnh; Quyết định 2853/QĐ-UBND ngày 05/9/2024 của UBND huyện về việc Quy định chức năng, nhiệm vụ, quyền hạn của Trung tâm Y tế huyện Cẩm Xuyên.

- Người đại diện: Nguyễn Phúc Long, Chức vụ: Giám đốc Trung tâm

- Địa chỉ: TDP 10, thị trấn Cẩm Xuyên, huyện Cẩm Xuyên, tỉnh Hà Tĩnh

- Thông tin liên hệ:

+ Số điện thoại: 0915.001.684

+ Email: longhoan.dr@gmail.com

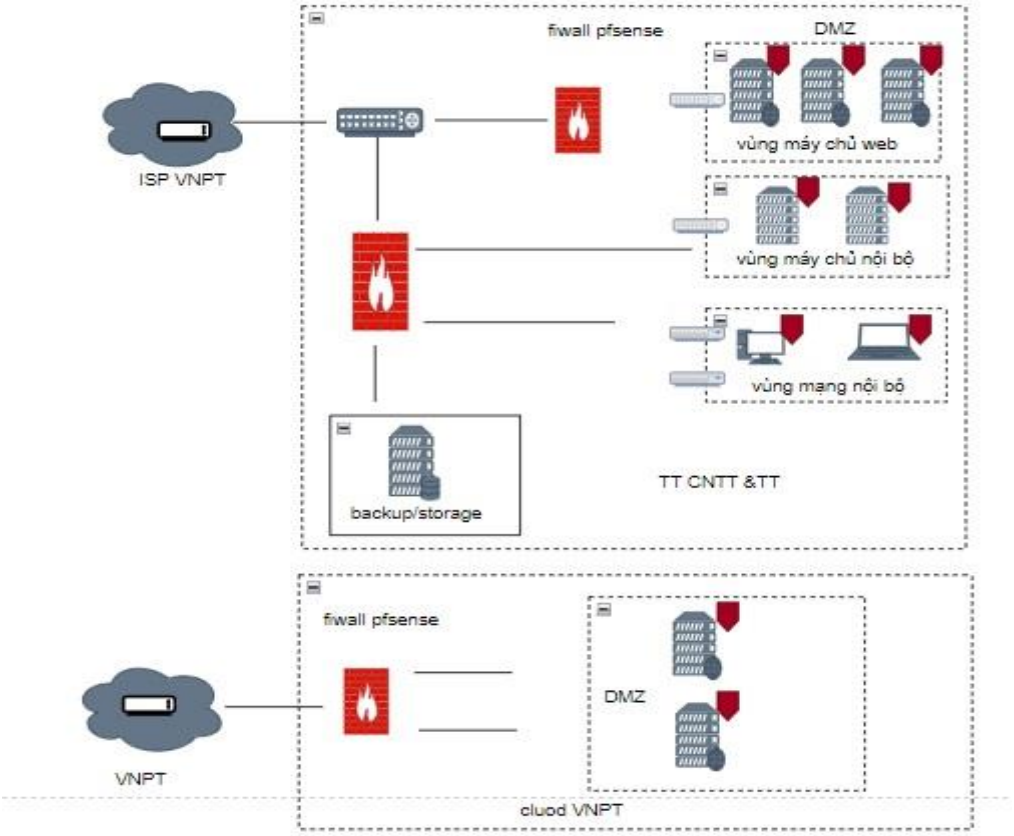
3. Mô tả phạm vi, quy mô của hệ thống

Phạm vi, quy mô của Hệ thống thông tin: Cổng thông tin điện tử Trung tâm y tế huyện Cẩm Xuyên: được thiết lập để phục vụ quảng bá hình ảnh và giao tiếp của Trung tâm y tế tới các tổ chức, doanh nghiệp và người dân

Đối tượng phục vụ của hệ thống: Tổ chức, cá nhân khác liên quan đến việc cung cấp thông tin hoạt động của Trung tâm y tế huyện Cẩm Xuyên

4. Mô tả cấu trúc của hệ thống

4.1. Mô hình logic tổng thể



Hình 1. Cấu trúc logic của hệ thống hiện tại

Các vùng mạng được thiết kế như sau:

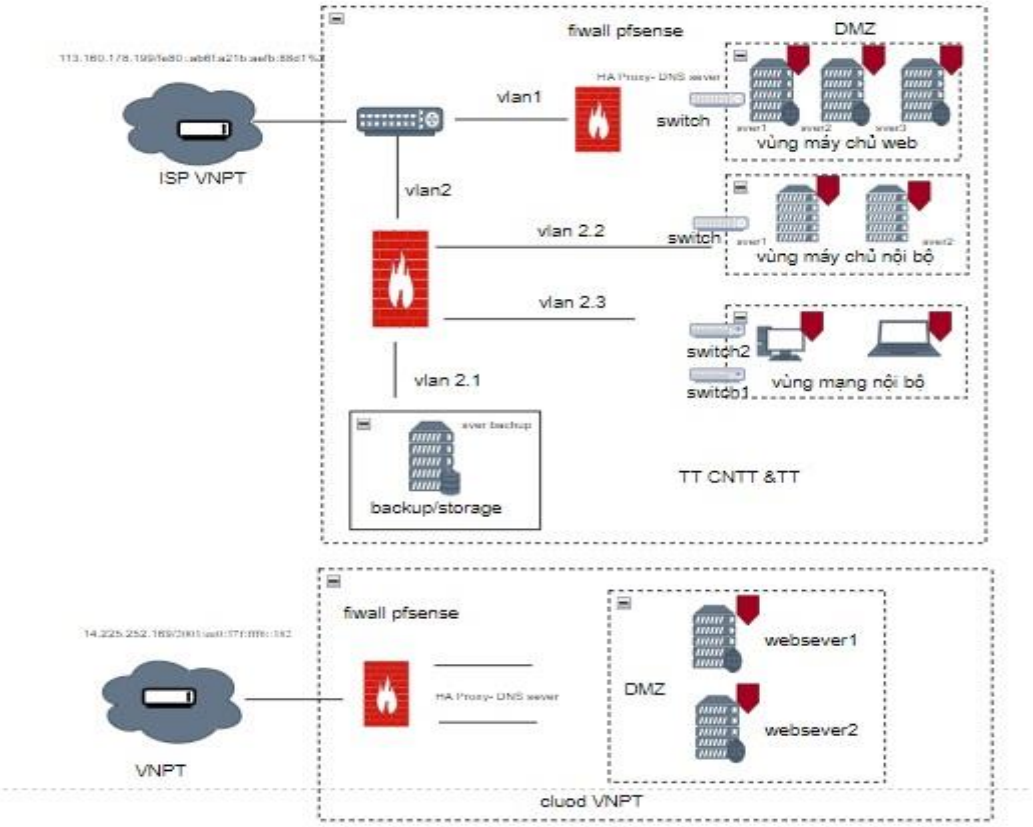
- Vùng mạng biên được đặt các thiết bị Router, Firewall để kết nối hệ thống ra các mạng bên ngoài và mạng Internet.

- Vùng DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet.

- Vùng máy chủ nội bộ (Server Farm) đặt các máy chủ nội bộ, máy chủ cơ sở dữ liệu, cung cấp các dịch vụ/chuyên ngành cho người sử dụng trong hệ thống.

- Vùng mạng nội bộ: Còn gọi là mạng LAN (Local area network), là nơi đặt các thiết bị mạng, máy trạm và máy chủ thuộc mạng nội bộ của đơn vị

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

a) Danh mục thiết bị mạng đang sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Router outsite/RGW	Vùng mạng biên	Kết nối và định tuyến động với các Router của ISP.
2	Router Mikrotik CCR1009-7G-1C-1S-1S+	Vùng mạng DMZ	Kết nối và định tuyến động với các Router của ISP.
2	Sisco catalyst 2960	Vùng máy chủ nội bộ	Kết nối các vùng mạng của hệ thống
3	Draytek vigorSwitch G2260	Vùng mạng nội bộ	Kết nối các máy trạm và thiết bị đầu cuối trong vùng mạng LAN.
4	Tplink TL-SG1016D	Vùng mạng nội bộ	Kết nối các máy trạm và thiết bị đầu cuối trong vùng mạng LAN.

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

b) Danh mục thiết bị tường lửa trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Firewall PfSence	Vùng mạng DMZ	Thiết bị tường lửa bảo vệ ứng dụng web.
2	Firewall Sico ASA 5510	Vùng mạng biên	Thiết bị tường lửa bảo vệ ứng dụng , website

Bảng 2. Danh mục thiết bị tường lửa trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Server Cenos7_HT1	Vùng máy chủ DMZ	Máy chủ cài đặt ứng dụng Web
2	Server VM_01	Vùng máy chủ DMZ	Máy chủ cài đặt ứng dụng Web
3	HP proliant DL380 gen 10(1)	Vùng máy chủ DMZ	Máy chủ cài đặt ứng dụng Web
4	Dell R730	Vùng máy chủ nội bộ	Lưu trữ CSDL của hệ thống
5	HP proliant DL380 gen 10(2)	Vùng máy chủ nội bộ	Lưu trữ CSDL của hệ thống

Bảng 3. Danh mục thiết bị máy chủ 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/Địa chỉ máy chủ cài đặt/Vùng mạng/HĐH	Mục đích sử dụng
1	Cổng thông tin điện tử Trung tâm Y tế huyện Cẩm Xuyên	ServerWindow/192.168.6.9 /113.160.178.199- fe80::ab6f:a21b:aefb:88d1%2	Máy chủ ứng dụng

Bảng 4. 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	Dải IP cho máy chủ vùng Application	192.168.0.65 192.168.0.136 192.168.0.159 192.168.10.1/24	14.225.252.183 113.160.178.199 fe80::ab6f:a21b:aefb:88d1%2 2001:ee0:37f:fff6::182
2	Dải IP cho vùng Database	192.168.6.1/24	Không public

Bảng 5. 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

TT	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống Cổng thông tin Trung tâm y tế huyện Cẩm Xuyên	1	Điều 7/NĐ85

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

Hệ thống Cổng thông tin Trung tâm y tế huyện Cẩm Xuyên được xây dựng để phục vụ quảng bá hình ảnh và giao tiếp của trung tâm y tế tới các tổ chức, doanh nghiệp và người dân. Đây là hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của Trung tâm y tế huyện Cẩm Xuyên, căn cứ theo quy định tại Điều 7 Nghị định 85/2016/NĐ-CP, 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 01 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 12 tháng,** kể từ khi HSĐXCĐ được phê duyệt.

Thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống Cổng thông tin trung tâm y tế huyện Cẩm Xuyên 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 Cổng thông tin trung tâm y tế huyện Cẩm Xuyên	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 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	**1. Quản lý an toàn mạng:** *(Tham chiếu Điều 10 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)* 1. 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. 2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng. 3. 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:** *(Tham chiếu Điều 11 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)* Quy định về quản lý an toàn máy chủ và ứng dụng: 1. Máy chủ phải được thiết lập chính sách xác thực và

	kiểm soát truy cập. Các hệ thống thông tin cần có phướng 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. 2. 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:** *(Tham chiếu Điều 12 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)* 1. 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. 2. 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. 3. 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:** *(Tham chiếu Điều 14 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)* Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm: 1. 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. 2. 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. 3. 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 4. Bộ phận 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. 5. Bộ phận 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. 6. Bộ phận 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 Điều 18 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	Quy chế này được Phòng Kế hoạch nghiệp vụ trình người đứng đầu đơn vị vận hành trước khi công bố áp dụng.

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 19 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	1. Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin,Văn phòng kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. 2. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sáchtrong quá trình triển khai, áp dụng chính sách an toàn thông tin./

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 16 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	1. Phòng Kế hoạch nghiệp vụ là bộ phận phối hợp với đơn vị chuyên trách về an toàn, an ninh thông tin huyện có trách nhiệm bảo đảm an toàn, an ninh cho các hệ thống thông tin. 2. Tuân thủ các quy định về trách nhiệm của bộ phận chuyên trách về an toàn thông tin được giao tại Quy chế này

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 5 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin: Trung tâm Y tế huyện Cẩm Xuyên giao phòng Kế hoạch

	nghiệp vụ là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống Hệ thống mạng nội bộ
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 5 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	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: a) Trung tâm y tế huyện Cẩm Xuyên - Người liên hệ: Nguyễn Thị Minh, công nghệ thông tin + Số điện thoại: 0915.877.286 + Email: nguyenminh0812@gmail.com b) UBND huyện Cẩm Xuyên + Họ và tên: Ngô Thị Tư, chuyên viên phòng Văn hóa - Thông tin; + Số điện thoại: 0972.633.602 + Email: ngothitu.cx@hatinh.gov.vn b) Sở Thông tin và Truyền thông tỉnh Hà Tĩnh Điện thoại: 02393606789 - Email: ttcntt-tt@hatinh.gov.vn - Địa chỉ: Số 18, đường 26/2, Thành phố Hà Tĩnh. - Thành viên thường trực: Ông Nguyễn Thanh Lâm - Phó Giám đốc Trung tâm Công nghệ thông tin và Truyền thông, Sở Thông tin và Truyền thông Hà Tĩnh. Điện thoại: 0914237788 Email: ntlam.stttt@hatinh.gov.vn c) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC) - Người liên hệ/bộ phận: Phòng Ứng cứu sự cố - Số điện thoại: 0869 100 317

	- Email: ir@vncert.vn - Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn - Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn

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 6 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên))*
Phương án	Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, 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 Điều 6 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên))*
Phương án	Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống: - Với người sử dụng: + Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. + Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT. + 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.

	- Với cán bộ quản lý và vận hành hệ thống + Cán bộ quản lý và vận hành hệ thống 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 quản lý và vận hành hệ thống 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 6 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	Định kỳ hàng năm tổ chức hoặc tham gia phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng do đơn vị chắc năng tổ chức.

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 6 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	Chấm dứt thay đổi công việc a) 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; b) Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi 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 7 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.
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 7 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

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 *(Tham chiếu Điều 8 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống. 2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi

	đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

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 9 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	1. 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. 2. Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng. 3. 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.

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 10 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	1. Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phướng 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. 2. 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…).

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 11 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	1. 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. 2. 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. 3. 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 quản lý rủi ro an toàn thông tin
Hiện trạng	Đáp ứng *(Tham chiếu Điều 13 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau: 1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống.

	2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản. 3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng.

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 14 Quy chế bảo đảm an toàn thông tin cho Hệ thống thông tin theo Quyết định số 73/QĐ-TTYT ngày 08 tháng 05 năm 2024 của Trung tâm y tế huyện Cẩm Xuyên)*
Phương án	Cá nhân hoặc tập thể có trách nhiệm bảo đảm an toàn thông tin mạng trong quản lý, sử dụng thiết bị công nghệ thông tin được giao. 1. Quy định hủy bỏ các thông tin/dữ liệu bảo mật Khi sửa chữa, khắc phục các sự cố của máy tính dùng soạn thảo văn bản mật, các phòng, đơn vị phải báo cáo cho người có thẩm quyền. Không được cho phép các tổ chức, cá nhân không có trách nhiệm trực tiếp sửa chữa, xử lý, khắc phục sự cố. 2. Quy định về xử lý và hủy bỏ phương tiện lưu trữ điện tử a) Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ chuyên trách về công nghệ thông tin kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành. b) Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi. 3. Quy định về xử lý thông tin trên các phương tiện và thiết bị CNTT: Trang thiết bị công nghệ thông tin có lưu trữ dữ liệu nhạy cảm khi thay đổi mục đích sử dụng hoặc thanh lý, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó đảm

	bảo không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị công nghệ thông tin đó. Trang thiết bị công nghệ thông tin có bộ phận lưu trữ dữ liệu hoặc thiết bị lưu trữ dữ liệu khi mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu)

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

Hệ thống thông tin: Hệ thống Cổng thông tin trung tâm y tế huyện Cẩm Xuyên được đề xuất là cấp độ 1. Do đó các thiết bị được sử dụng để triển khai hệ thống và các thành phần khác trong hệ thống như hạ tầng mạng, hệ thống lưu trữ… được thuyết minh phương án đáp ứng yêu cầu cấp độ 1 như sau:

6.2.1. Bảo đảm an toàn mạng

6.2.1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng nội bộ	Có	Hệ thống ứng dụng được thiết kế tách biệt với các hệ thống dịch vụ khác. Việc phân các vùng chức năng được thực hiện trên Tường Firewall PfSence, Firewall Sico ASA 5510
2	Vùng mạng biên	Có	
3	Vùng DMZ	Có	
4	Vùng máy chủ nội bộ	Có	

b) Phương án bảo đảm an toàn thông tin

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	Sử dụng Tường lửa Firewall PfSence có tích hợp chức năng VPN để quản lý truy cập, quản trị hệ thống từ xa an toàn. Tính năng VPN này được cấu hình trực tiếp trên thiết bị Firewall PfSence, Firewall Sico ASA 5510 quản lý truy cập từ bên ngoài vào vùng mạng nội bộ , từ bên ngoài vào vùng máy chủ nội bộ, từ vùng mạng nội bộ vào vùng máy chủ nội bộ

2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc sản phẩm chống tấn công, xâm nhập	Có	Sử dụng Tường lửa Firewall PfSence, Firewall Sico ASA 5510 có tích hợp chức năng IPS để quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập. Tính năng IPS được cấu hình trên Firewall PfSence, Firewall Sico ASA 5510 kiểm soát truy cập và phòng chống xâm nhập giữa các phân vùng mạng nội bộ, máy chủ nội bộ và phân vùng mạng DMZ.
3	Phương án phòng chống mã độc cho máy chủ và máy trạm	Có	Sử dụng sản phẩm Phòng chống mã độc Bkav Endpoint AI
4	Phương án phòng chống tấn công mạng cho ứng dụng web	Có	Sử dụng sản phẩm Tường lửa Firewall PfSence, Firewall Sico ASA 5510 được đặt tại phân vùng mạng DMZ
5	Phương án dự phòng cho các thiết bị mạng chính	Có	Hạ tầng mạng đều được xây dựng ảo hóa trên hệ thống cluod VNPT, hệ thống tường lửa tại Trung tâm CNTT và Truyền thông luôn được dự phòng bằng Firewall PfSence

6.2.1.2. 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 sử dụng Tường lửa Firewall PfSence, Firewall Sico ASA 5510 có tích hợp chức năng VPN 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.

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	Tường lửa Firewall PfSence, Firewall Sico ASA 5510 được thiết lập chỉ cho phép 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
3	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.	Có	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng trên Tường lửa Firewall PfSence, Firewall Sico ASA 5510 và ngắt phiên kết nối VPN khi người dùng không thao tác sử dụng trong 1 khoảng thời gian

6.2.1.3 Kiểm soát truy cập từ bên trong mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức	Có	Chính sách kiểm soát truy cập từ các vùng mạng trong hệ thống đi ra các mạng bên ngoài và mạng Internet được thiết lập trên Tường lửa Firewall PfSence, Firewall Sico ASA 5510

6.2.1.4. Nhật ký hệ thống

Yêu cầu **Thiết bị**	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống	Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian
Router outsite/RGW	+	+
Firewall Sico ASA 5510	+	+
Firewall PfSence	+	+

6.2.1.5. Phòng chống xâm nhập

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống	Đáp ứng	Sử dụng Tường lửa Firewall PfSence, Firewall Sico ASA 5510 có tích hợp chức năng IPS để bảo vệ các vùng mạng trong hệ thống. Tính năng IPS được cấu hình trên Firewall PfSence kiểm soát truy cập và phòng chống xâm nhập giữa các phân vùng mạng nội bộ, máy chủ nội bộ và phân vùng mạng DMZ.
2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng	Đáp ứng	Thực hiện định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng trên Tường lửa Firewall PfSence. Firewall Sico ASA 5510

6.2.1.6. Bảo vệ thiết bị hệ thống

Yêu cầu **Thiết bị**	Cấu hình chức năng xác thực trên các thiết bị	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa	Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa
Router outsite/RGW	+	+	+
Firewall PfSence	+	+	+
Firewall Sico ASA 5510	+	+	+
Bkav Endpoint AI	+	+	+

6.2.2. Bảo đảm an toàn máy chủ

6.2.2.1. Xác thực

Yêu cầu	Thiết lập chính sách xác thực trên máy chủ	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập chính sách mật khẩu an toàn: Yêu cầu thay đổi mật khẩu mặc định; Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ
Máy chủ			
Server Window/192.168.6.9 /113.160.178.199- fe80::ab6f:a21b:aefb:88d1%2	+	+	+

6.2.2.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)
Máy chủ		
Server Window/192.168.6.9 /113.160.178.199- fe80::ab6f:a21b:aefb:88d1%2	+	+

6.2.2.3. 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	Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng
Máy chủ			
Server Window/192.168.6.9 /113.160.178.199-	+	+	+

fe80::ab6f:a21b:aefb:88d1%2			

6.2.2.4. 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	Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng	Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng
Máy chủ				
Server Window/192.168.6.9 /113.160.178.199-fe80::ab6f:a21b:aefb:88d1%2	+	+	+	+

6.2.2.5. Phòng chống phần mềm độc hại

Yêu cầu	Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật	Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt
Máy chủ		
Server Window/192.168.6.9 /113.160.178.199-fe80::ab6f:a21b:aefb:88d1%2	+	+

6.2.2.6. Xử lý máy chủ khi chuyển giao

STT	**Yêu cầu**	**P/A**	**Ghi chú/Mô tả**
1	Có phương án xóa sạch thông	Đáp	Hiện tại chưa có phương án

	tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	ứng	chuyển giao cho đơn vị sử dụng. Sẽ có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng

6.2.3. Bảo đảm an toàn ứng dụng

6.2.3.1. Xác thực

Yêu cầu / **Ứng dụng**	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	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
Hệ thống Cổng thông tin Trung tâm y tế huyện Cẩm Xuyên	+	+	+	+

6.2.3.2. Kiểm soát truy cập

Yêu cầu / **Ứng dụng**	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	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa
Hệ thống Cổng	+	+	+

thông tin Trung tâm y tế huyện Cẩm Xuyên			

6.2.3.3. 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; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng.	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng
Ứng dụng		
Hệ thống Cổng thông tin trung tâm y tế huyện Cẩm Xuyên	+	+

6.2.3.4. An toàn ứng dụng và mã nguồn

Yêu cầu	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
Ứng dụng	
Hệ thốngCổng thông tin trung tâm y tế huyện Cẩm Xuyên	+

6.2.4. Bảo đảm an toàn dữ liệu

6.2.4.1. Bảo mật dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin,	Có	Thiết lập mã hóa dữ liệu trên thiết bị lưu trữ, phương tiện

	dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ		lưu trữ.

6.2.4.2. 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 cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ	Có	Có thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ trên ổ cứng di động