

SỞ Y TẾ TỈNH CÀ MAU
BỆNH VIỆN LAO VÀ BỆNH PHỔI CÀ MAU



**HỒ SƠ ĐỀ XUẤT CẤP ĐỘ
HỆ THỐNG QUẢN LÝ VÀ ĐIỀU HÀNH
THÔNG TIN TẠI BỆNH VIỆN LAO VÀ BỆNH
PHỔI CÀ MAU**

Cà Mau – 2025

MỤC LỤC

MỤC LỤC	1
THUẬT NGỮ, TỪ VIẾT TẮT	1
DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ	1
PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN	2
1. Thông tin Chủ quản hệ thống thông tin	2
2. Thông tin Đơn vị vận hành	2
3. Mô tả phạm vi, quy mô của hệ thống	2
4. Mô tả cấu trúc của hệ thống	3
PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT	8
1. Danh mục hệ thống thông tin và cấp độ đề xuất	8
2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin	8
PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN	9
PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 2	11
1. Thiết lập chính sách an toàn thông tin	11
2. Tổ chức bảo đảm an toàn thông tin	13
3. Bảo đảm nguồn nhân lực	15
4. Quản lý thiết kế, xây dựng hệ thống thông tin	17
5. Quản lý vận hành hệ thống thông tin	21

PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÀNH PHẦN CẤP ĐỘ 2

30

1. Bảo đảm an toàn mạng

30

2. Bảo đảm an toàn máy chủ

33

3. Bảo đảm an toàn ứng dụng

37

4. Bảo đảm an toàn dữ liệu

39

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	HSDXCĐ	Hồ sơ đề xuất cấp độ
4	LAN	Mạng nội bộ
5	WAN	Mạng tin học diện rộng
6	VPN	Vitural Private Network
7	DMZ	Vùng mạng phi quân sự

DANH MỤC CÁC BẢNG

Bảng 1. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống	7
Bảng 2. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống	7

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

Hình 1. Cấu trúc logic của hệ thống	3
Hình 2. Kết nối vật lý của hệ thống	4

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

41. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: Bệnh viện Lao và Bệnh phổi Cà Mau
- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 0941/QĐ-UBND, ngày 05 tháng 9 năm 2025 của Ủy ban nhân dân tỉnh Cà Mau về việc quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bệnh viện Lao và Bệnh phổi Cà Mau thuộc Sở Y tế tỉnh Cà Mau.
- Người đại diện: **Trần Quang Dũng** ; chức vụ: Phó Giám đốc phụ trách điều hành
- Địa chỉ: Số 100, đường Hải Thượng Lãn Ông, phường Hòa Thành, tỉnh Cà Mau
- Thông tin liên hệ: Số điện thoại: 02903 688 988

42. Thông tin Đơn vị vận hành

- Tên đơn vị vận hành: Tổ công nghệ thông tin
- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 60/QĐ-BVLBP ngày 09/9/2025 của Bệnh viện Lao và Bệnh phổi Cà Mau thành lập tổ Công nghệ thông tin thuộc Bệnh viện Lao và Bệnh phổi Cà Mau.
- Người đại diện: **Bùi Hữu Thái** ; Chức vụ: Nhân viên
- Địa chỉ: Số 100, đường Hải Thượng Lãn Ông, phường Hòa Thành, tỉnh Cà Mau
- Thông tin liên hệ: Số điện thoại: 0913578071

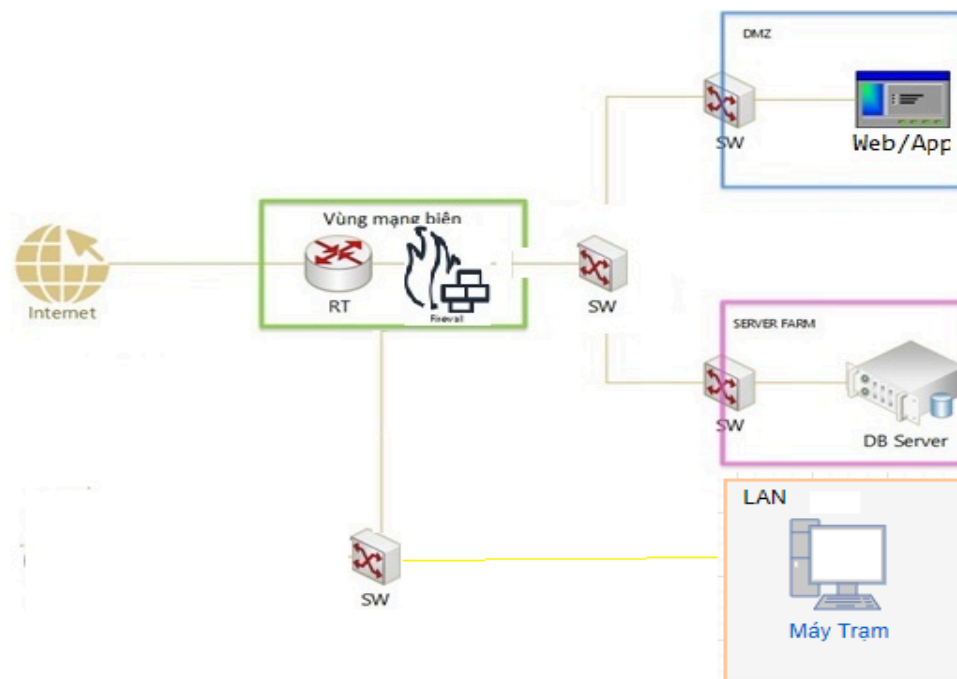
43. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống thông tin: Hệ thống thông tin phục vụ hoạt động nội bộ của Bệnh viện và có xử lý thông tin riêng, thông tin cá nhân của người dùng nhưng không xử lý thông tin bí mật của nhà nước; hệ thống cơ sở hạ tầng công nghệ thông tin phục vụ hoạt động của Bệnh viện.
- Đối tượng phục vụ của hệ thống: Cán bộ, nhân viên y tế, người lao động của Bệnh viện và người bệnh.
- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi Hệ thống:
 - + Phần mềm quản lý bệnh viện (HIS)

- + Hệ thống quản lý xét nghiệm (LIS)
- + Hệ thống chẩn đoán hình ảnh (PACS)
- + Hệ thống Quản lý văn bản và Điều hành
- + Bệnh án điện tử (EMR)
- + Hệ thống chữ ký số
- + Cơ sở hạ tầng công nghệ thông tin

44. Mô tả cấu trúc của hệ thống

44.1. Sơ đồ logic tổng thể

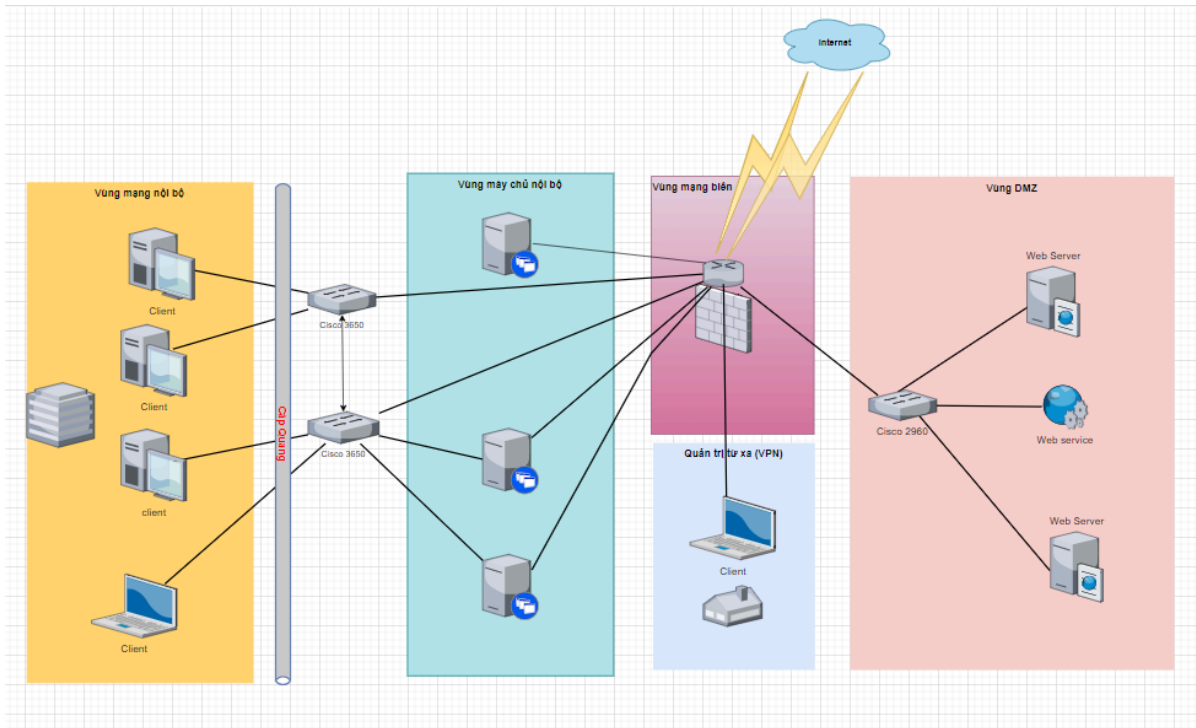


Hình 1. Cấu trúc logic của hệ thống

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 LAN: đặt các máy trạm và các thiết bị ngoại vi để kết nối hệ thống dịch vụ của Bệnh viện, truy cập mạng Internet.

44.2. Sơ đồ kết nối vật lý



Hình 2. Kết nối vật lý của hệ thống

44.3. Danh mục thiết bị sử dụng trong hệ thống

ST T	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Router Microtik	Vùng mạng biên	Kết nối hệ thống với các mạng bên ngoài; làm mất toàn bộ kết nối tới các mạng bên ngoài hệ thống khi gặp sự cố
2	Firewall (Microtik có tính năng tường lửa)	Vùng mạng biên	Quản lý truy cập vào/ra và bảo vệ vùng DMZ; Vùng máy chủ nội bộ.
3	SW Cisco2960	Vùng mạng DMZ	Thiết bị định tuyến kết nối vùng DMZ
4	SW Cisco3650	Vùng máy chủ nội bộ	Thiết bị định tuyến quản lý, kết nối vùng máy chủ nội bộ

5	SW Cisco2960	Vùng mạng biên	Thiết bị định tuyến quản lý, kết nối đến các vùng máy chủ nội bộ, vùng DMZ
6	SW/Cisco2960	Vùng mạng tại các toà nhà	Thiết bị định tuyến quản lý, kết nối đến các vùng máy chủ nội bộ, vùng DMZ
7	WebServer (máy chủ vật lý)	Vùng mạng DMZ	Máy chủ cài đặt ứng dụng Web
8	Database Server (máy chủ ảo và máy chủ vật lý)	Vùng máy chủ nội bộ	Lưu trữ CSDL của hệ thống

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

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

ST T	Tên dịch vụ	Máy chủ/Ứng dụng cài đặt/Vùng mạng/HĐH	Mục đích sử dụng
1	Phần mềm đặt lịch khám bệnh Online	Web Server (Vật lý)/Cài đặt Web-App/Vùng DMZ/Window Server 2016 Database Server (Máy Ảo)/ Cài đặt Oracle server 11gR2/Vùng máy chủ nội bộ/Linux	Cài đặt phần mềm đăng kí khám bệnh Online
2	Phần mềm quản lý bệnh viện (HIS)	App Server (Máy ảo)/Cài đặt App/Vùng máy chủ nội bộ/Window Server 2019 Database Server (Máy Ảo)/ Cài đặt Oracle server 11gR2/Vùng máy chủ nội bộ/Linux	Cài đặt phần mềm quản lý bệnh viện phục vụ công tác khám chữa bệnh cho người bệnh
3	Hệ thống quản lý xét nghiệm (LIS)	App Server (Máy ảo)/Cài đặt App/Vùng máy chủ nội bộ/Window Server 2016	Quản lý xét nghiệm phục vụ công tác khám chữa bệnh

		Database Server (Máy Ảo)/ Cài đặt SQL Server 2014/Vùng máy chủ nội bộ/Linux	
4	Hệ thống chẩn đoán hình ảnh (PACS)	Web Server (Máy ảo)/Cài đặt Web-App/Vùng DMZ/Ubuntu 18.04 Database Server (Máy Ảo)/ Cài đặt Mysql mariadb Server 10/Vùng máy chủ nội bộ/Ubuntu 18.04	Quản lý hệ thống hình ảnh phục vụ công tác khám chữa bệnh
5	Hệ thống Quản lý văn bản và Điều hành	Web Server (Vật lý)/Cài đặt Web-App/Vùng máy chủ nội bộ/Windows Server 2012 Database Server (Vật lý)/ Cài đặt IBM Domino Server/Vùng máy chủ nội bộ/Windows Server 2012	Phục vụ công tác quản lý, điều hành và xử lý văn bản tại Bệnh viện
6	Phần mềm quản lý chấm công vân tay	App Server (Máy ảo)/Cài đặt App/Vùng máy chủ nội bộ/Windows Server 2019 Database Server (Máy ảo)/ Cài đặt PostgreSQL Server/Vùng máy chủ nội bộ/Windows Server 2019	Phục vụ công tác quản lý chấm công và tính lương cho nhân viên
7	Bệnh án điện tử (EMR)	App Server (Máy ảo)/Cài đặt App/Vùng máy chủ nội bộ/Window Server 2019 Database Server (Máy Ảo)/ Cài đặt Oracle server 11gR2/Vùng máy chủ nội bộ/Linux	Hồ sơ bệnh án được hiển thị và lưu trữ bằng phương tiện điện tử (đang triển khai thử nghiệm tại 03 khoa)
8	Hệ thống chữ ký số	App Server (Máy ảo)/Cài đặt App/Vùng máy chủ nội bộ/CentOS Linux 7	Sử dụng thay thế chữ ký tay trong công tác khám chữa bệnh và thanh toán viện phí

		Database Server (Máy Ảo)/ Cài đặt MySQL Server/Vùng máy chủ nội bộ/CentOS Linux 7	
9	Hệ thống mạng nội bộ - LAN của Bệnh viện		Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của Bệnh viện
10	Phòng máy chủ		Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của Bệnh viện

Bảng 1. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

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

STT	Vùng mạng	IP Private	IP Public
1	Vùng máy DMZ		
2	Vùng máy chủ nội bộ		
3	Vùng mạng biên		
4	Vùng mạng nội bộ		

Bảng 2. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

STT	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Phần mềm quản lý bệnh viện (HIS)	2	Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP
2	Hệ thống quản lý xét nghiệm (LIS)	2	Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP
3	Hệ thống chẩn đoán hình ảnh (PACS)	2	Khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP
4	Hệ thống Quản lý văn bản và Điều hành	2	Khoản 1, Điều 8 Nghị định số 85/2016/NĐ-CP
5	Bệnh án điện tử (EMR)	2	Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP
6	Hệ thống chữ ký số	2	Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP
7	Hệ thống mạng nội bộ - LAN của Bệnh viện	2	Khoản 3 Điều 8 Nghị định 85/2016/NĐ-CP
8	Phòng máy chủ	2	Khoản 3 Điều 8 Nghị định 85/2016/NĐ-CP

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

Hệ thống quản lý và điều hành thông tin tại Bệnh viện được xây dựng để phục vụ hoạt động của Bệnh viện: trao đổi, quản lý, điều hành, phục vụ công tác khám chữa bệnh, xử lý công việc trên môi trường mạng. Căn cứ theo quy định tại Khoản 1, 2, 3 Điều 8 Nghị định 85/2016/NĐ-CP, hệ thống này được đề xuất cấp độ 2.

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

I. 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
 - Quản lý sự cố an toàn thông tin
 - Quản lý an toàn người sử dụng đầu cuối.
6. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

II. 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. Kiểm soát truy cập từ bên trong mạng
 - 1.4. Nhật ký hệ thống
 - 1.5. Phòng chống xâm nhập
 - 1.6. 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

2.6. Xử lý máy chủ khi chuyển giao

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

3.2. Kiểm soát truy cập

3.3. Nhật ký hệ thống

3.4. An toàn ứng dụng và mã nguồn

4. Bảo đảm an toàn dữ liệu

4.1. Bảo mật dữ liệu

4.2. Sao lưu dự phòng

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống quản lý và điều hành thông tin bệnh viện sẽ bao gồm các thuyết minh thành phần sau:

ST T	Hệ thống	Cấp độ đề xuất	Nội dung thuyết minh
1	Thuyết minh phương án đáp ứng yêu cầu quản lý	2	Phụ lục I
2	Thuyết minh phương án đáp ứng yêu cầu kỹ thuật	2	Phụ lục II

**PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN
THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 2**

61. Thiết lập chính sách an toàn thông tin

61.1. Chính sách an toàn thông tin

Yêu cầu	Xây dựng chính sách an toàn thông tin
Hiện trạng	Bệnh viện thực hiện theo Quy chế Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng CNTT của ngành y tế tỉnh Cà Mau (được Bệnh viện Lao – Bệnh phổi Cà Mau ban hành tại Quyết định số 06/QĐ-BVLBP ngày 01/8/2025).
Phương án	1. Quản lý an toàn mạng: a) Hệ thống mạng 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 LAN được bảo vệ bằng tường lửa (tích hợp tường lửa trên thiết bị cân bằng tải Mikrotik) và phân chia hệ thống mạng thành các VLAN 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 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 tạm thời 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, CSDL; 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) Phòng KH-TC 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) Phòng KH-TC huỷ bỏ quyền truy cập vào hệ thống thông tin, thu hồi lại tất cả các tài sản liên quan tới hệ thống thông tin của Bệnh viện (khoá, thẻ nhận dạng, thư mục lưu trữ, thư điện tử công vụ, máy vi tính, tài khoản truy cập hệ thống) khi cán bộ, viên chức và người lao động chuyển công tác, nghỉ hưu hoặc chấm dứt lao động hợp đồng.
--	--

	f) Phòng KH-TC 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.
--	---

61.2. Xây dựng và công bố

Yêu cầu	Quy định về xây dựng và công bố Quy chế bảo đảm an toàn thông tin
Hiện trạng	Bệnh viện thực hiện theo Quy chế Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng CNTT của ngành y tế tỉnh Cà Mau (được Bệnh viện Lao – Bệnh phổi Cà Mau ban hành tại Quyết định số 06/QĐ-BVLBP ngày 01/8/2025).
Phương án	Sở Y tế tỉnh Cà Mau đã xây dựng và công bố Quy chế bảo đảm an toàn thông tin cho ngành y tế Cà Mau

61.3. Rà soát, sửa đổi

Yêu cầu	Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin
Hiện trạng	Quy chế Bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng CNTT của ngành y tế tỉnh Cà Mau (được Bệnh viện Lao – Bệnh phổi Cà Mau ban hành tại Quyết định số 06/QĐ-BVLBP ngày 01/8/2025).
Phương án	Rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin: 1. Định kỳ hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. 2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Văn phòng Sở Y tế để tổng hợp báo cáo Lãnh đạo sở xem xét điều chỉnh, bổ sung.

62. Tổ chức bảo đảm an toàn thông tin

62.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Phòng KH-TC chuyên trách về an toàn thông tin tại Bệnh viện Lao và Bệnh phổi Cà Mau
----------------	---

Hiện trạng	Bộ phận chuyên trách về an toàn thông tin (<i>Tham chiếu điều 16 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau</i>)
Phương án	Giao Phòng KH-TC là bộ phận chuyên trách về ATTT cho Hệ thống quản lý và điều hành thông tin tại Bệnh viện Lao và Bệnh phổi Cà Mau

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

62.2.1. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin

Yêu cầu	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	Tham chiếu Điều 16 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế tỉnh Cà Mau
Phương án	Bệnh viện Đa khoa tỉnh giao Phòng Công nghệ thông tin là đầu mối liên hệ, phối hợp với Sở Y tế, Công an tỉnh, Sở Thông tin và Truyền về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống quản lý và điều hành thông tin tại Bệnh viện Lao và Bệnh phổi Cà Mau

62.2.2. 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

Yêu cầu	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	Tham chiếu Điều 16 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau
Phương án	Phòng KH-TC làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của Hệ thống thông tin.

11.1.1. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền

Yêu cầu	Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 15 và Điều 16 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau)</i>
Phương án	Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền

12. Bảo đảm nguồn nhân lực

12.1. Tuyển dụng

Yêu cầu	Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ
Hiện trạng	Đáp ứng một phần <i>(Đã có cán bộ chuyên trách bảo đảm an toàn thông tin mạng của Bệnh viện. Tuy nhiên, trong Quyết định tuyển dụng hoặc hợp đồng lao động chưa có quy định trách nhiệm)</i>
Phương án	Bổ sung Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng: a) Quy định 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. b) Có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng.

12.2. Trong quá trình làm việc

12.2.1. 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

Yêu cầu	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 <i>(Tham chiếu Điều 15 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
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 cán bộ quản lý và vận hành hệ thống a) 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. b) 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. c) Các cơ quan, địa phương và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên hệ thống.

12.2.2. Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng

Yêu cầu	Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng
Hiện trạng	Đáp ứng

Phương án	- Cử cán bộ chuyên trách CNTT tham gia các chương trình diễn tập, tập huấn về an toàn thông tin do các cơ quan chức năng tổ chức. - Các thông tin tuyên truyền, phổ biến kiến thức về an toàn thông tin phải được phổ biến đến 100% cán bộ, viên chức và người lao động trong cơ quan trên Phần mềm Quản lý văn bản và Điều hành.
------------------	--

12.3. Chấm dứt hoặc 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.

Yêu cầu	Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc
Hiện trạng	Đáp ứng
Phương án	- Cán bộ, viên chức, người lao động nghỉ việc hoặc thay đổi công việc phải thu hồi các tài khoản, quyền truy cập hệ thống, các trang thiết bị, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của Bệnh viện. - Phòng Tổ chức cán bộ, Trưởng các phòng, khoa, trung tâm có trách nhiệm phối hợp với Phòng KH-TC trong việc thu hồi tài sản, tài khoản, quyền truy cập của cán bộ, viên chức và người lao động nghỉ việc hoặc thay đổi công việc.

b) Có quy trình và 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.

Yêu cầu	Có quy trình và 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.
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 8 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

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

13.1. Thiết kế an toàn hệ thống thông tin

13.1.1. 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	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 <i>(Tham chiếu Điều 2, Điều 6, Điều 8 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Thiết kế an toàn hệ thống thông tin Yêu cầu phải có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

13.1.2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin

Yêu cầu	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin
Hiện trạng	Tham chiếu Điều 2, Điều 6, Điều 8 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau.
Phương án	Tham mưu Lãnh đạo bệnh viện phê duyệt tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

13.1.3. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ

Yêu cầu	Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ
Hiện trạng	Đáp ứng
Phương án	Phương án bảo đảm an toàn thông tin theo cấp độ được mô tả tại Phụ lục II tài liệu này.

13.1.4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin

Yêu cầu	Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin
Hiện trạng	Tham chiếu Điều 8, Điều 9, Điều 10, Điều 11, Điều 12 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau.
Phương án	Tham mưu Lãnh đạo bệnh viện phê duyệt tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

13.1.5. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống

Yêu cầu	Có quy định khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống
Hiện trạng	Đáp ứng (Tham chiếu Điều 6, Điều 7 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).
Phương án	Thiết kế an toàn hệ thống thông tin Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

13.2. Phát triển phần mềm thuê khoán

13.2.1. Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán

Yêu cầu	Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán
Hiện trạng	Đáp ứng
Phương án	Quy định đối với việc phát triển phần mềm thuê khoán:

	Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán.
--	---

13.2.2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm

Yêu cầu	Có quy định yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm
Hiện trạng	Đáp ứng
Phương án	Quy định đối với việc phát triển phần mềm thuê khoán: Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

13.3. Thử nghiệm và nghiệm thu hệ thống

13.3.1. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng

Yêu cầu	Có thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng
Hiện trạng	Đáp ứng
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng.

13.3.2. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có yêu cầu về nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng một phần
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống:

	Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống. Bổ sung quy trình thử nghiệm và nghiệm thu hệ thống tại dự thảo <i>Quy chế thử nghiệm và nghiệm thu hệ thống</i> trong vòng 06 tháng kể từ khi HSDXCD được phê duyệt.
--	---

13.3.3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.

14. Quản lý vận hành hệ thống thông tin

14.1. Quản lý an toàn mạng

14.1.1. Quản lý, vận hành hoạt động bình thường của hệ thống

Yêu cầu	Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 6, Điều 7, Điều 8, Điều 9, Điều 10 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>

Phương án	Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn. b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có. c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm. d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp. e) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng. f) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.
------------------	---

14.1.2. Cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố

Yêu cầu	Có quy định về cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố
Hiện trạng	Tham chiếu Điều 10 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế tỉnh Cà Mau.
Phương án	Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: Triển khai hệ thống và phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, CSDL; dữ liệu, thông tin nghiệp vụ.

14.1.3. Truy cập và quản lý cấu hình hệ thống

Yêu cầu	Truy cập và quản lý cấu hình hệ thống
Hiện trạng	Đáp ứng

	<i>(Tham chiếu Điều 8 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Truy cập và quản lý cấu hình hệ thống: Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại Trung tâm dữ liệu theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

14.2. Quản lý an toàn máy chủ và ứng dụng

Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:

14.2.1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ

Yêu cầu	Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 9, Điều 10 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ: a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn. b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có. c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm. d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp. đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng. e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

14.2.2. Truy cập mạng của máy chủ

Yêu cầu	Có quy định quản lý truy cập mạng của máy chủ
Hiện trạng	Đáp ứng
Phương án	Truy cập mạng của máy chủ: Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng như bên ngoài vào hệ thống.

14.2.3. Truy cập và quản trị máy chủ và ứng dụng

Yêu cầu	Có quy định quản lý truy cập và quản trị máy chủ và ứng dụng
Hiện trạng	Đáp ứng
Phương án	Truy cập và quản trị máy chủ và ứng dụng: a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng. b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành. c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

14.2.4. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

Yêu cầu	Có quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 10 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>

Phương án	Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, CSDL; dữ liệu, thông tin nghiệp vụ.
------------------	--

14.3. Quản lý an toàn dữ liệu

14.3.1. Chính sách, quy trình dự phòng và khôi phục dữ liệu

Yêu cầu	Có chính sách, quy trình dự phòng và khôi phục dữ liệu
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 10 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Yêu cầu an toàn đối với phương pháp mã hóa a) Bệnh viện áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin. b) Có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa. 2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa. 3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu. 4. Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ.

14.3.2. 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

Yêu cầu	Có quy định 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, CSDL; dữ liệu, thông tin nghiệp vụ
Hiện trạng	Đáp ứng.
Phương án	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, CSDL; dữ liệu, thông tin nghiệp vụ. Bản sao lưu được lưu trữ tối thiểu thành 02 bản và được lưu trữ ở hai địa chỉ khác nhau.

14.4. Quản lý sự cố an toàn thông tin

14.4.1. Phân nhóm sự cố an toàn thông tin mạng

Yêu cầu	Có quy định về phân nhóm sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 12 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm: a) Thấp: sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của đơn vị: máy tính trạm bị nhiễm phần mềm độc hại, phần mềm hệ điều hành, các phần mềm ứng dụng cài đặt trên máy tính cá nhân phát sinh lỗi; b) Trung bình: sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị: hệ thống mạng của 1 (một) khoa, phòng, ban, trung tâm thuộc đơn vị bị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 khoa, phòng, ban, trung tâm; c) Cao: sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và có ảnh hưởng đến hoạt động của đơn vị: hệ thống quản lý văn bản và điều hành, hồ sơ cấp phép, một cửa điện tử của đơn vị bị ngưng hoạt động, một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tập tin chung,) bị hư hỏng;

	d) Khẩn cấp: sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của đơn vị: toàn bộ hệ thống thiết bị công nghệ thông tin, hệ thống cung cấp điện ngừng hoạt động, hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung...
--	---

14.4.2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng

Yêu cầu	Có phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 12 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 12 Quyết định số 1361/QĐ-SYT.

14.4.3. Kế hoạch ứng phó sự cố an toàn thông tin mạng

Yêu cầu	Xây dựng kế hoạch ứng phó sự cố an toàn thông tin mạng
Hiện trạng	Tham chiếu Khoản 3,4 Điều 12 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau.
Phương án	Phòng KH-TC tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin.

14.4.4. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

Yêu cầu	Có quy định về quản lý giám sát, phát hiện và cảnh báo sự cố an toàn thông tin
Hiện trạng	Đáp ứng.

	<i>(Tham chiếu Điều 12 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Có phương án và điều động nhân lực có kinh nghiệm thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh báo sớm về nguy cơ mất ATTT trong hệ thống. Đối với người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của Bệnh viện khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

14.4.5. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường

Yêu cầu	Có quy trình ứng cứu sự cố an toàn thông tin mạng thông thường
Hiện trạng	Đáp ứng <i>(Tham chiếu Khoản 4, Điều 12 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Phòng KH-TC có trách nhiệm tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin.

14.4.6. Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng

Yêu cầu	Có quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 12 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Phòng KH-TC có trách nhiệm tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin.

14.4.7. Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin

Yêu cầu	Có quy định về cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 12 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến hệ thống

14.5. Quản lý an toàn người sử dụng đầu cuối

14.5.1. Quản lý truy cập, sử dụng tài nguyên nội bộ

Yêu cầu	Có quy định về quản lý truy cập, sử dụng tài nguyên nội bộ
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 8 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Quản lý truy cập, sử dụng tài nguyên nội bộ: a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của Bệnh viện. b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của Phòng KH-TC. c) Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống.

14.5.2. Quản lý truy cập mạng và tài nguyên trên Internet

Yêu cầu	Có quy định về quản lý truy cập mạng và tài nguyên trên Internet
Hiện trạng	Đáp ứng <i>(Tham chiếu Điều 7, 8, 15 Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin ngành y tế Cà Mau).</i>
Phương án	Quản lý truy cập mạng và tài nguyên trên Internet: a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao. b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng. c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và Phòng KH-TC để kịp thời ngăn chặn và xử lý. d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức. e) Không truy cập vào các hệ thống thông tin công cộng không rõ về nội dung hoặc có nội dung phản cảm, không phù hợp với thuần phong mỹ tục của Việt Nam. Không đọc thư điện tử hoặc tải tệp tin đính kèm trong thư không rõ người gửi; Không kích hoạt các đường liên kết có dấu hiệu không rõ ràng.

PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÀNH PHẦN CẤP ĐỘ 2

Hệ thống thông tin: Quản lý và điều hành thông tin tại Bệnh viện Lao và Bệnh phổi Cà Mau được đề xuất là cấp độ 2. Do đó, các máy chủ 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 2 như sau:

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống:

ST T	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng nội bộ(LAN)	Có	Là vùng đặt các máy trạm và các thiết bị ngoại vi
2	Vùng mạng biên	Có	Kết nối hệ thống với mạng Internet và mạng diện rộng
3	Vùng DMZ	Có	Đặt máy chủ WEBAPP, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet.
4	Vùng máy chủ nội bộ	Có	Là vùng đặt máy chủ cơ sở dữ liệu.

b) Phương án bảo đảm an toàn thông tin

ST T	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 Generic Firewall có tích hợp chức năng VPN để quản lý truy cập, quản trị hệ thống từ xa an toàn.
2	Phương án quản lý truy cập giữa các	N/A	Sử dụng Tường lửa Generic Firewall có tích hợp chức năng IPS để quản lý truy cập

	vùng mạng và phòng chống xâm nhập		giữa các vùng mạng và phòng chống xâm nhập.
3	Phương án dự phòng cho các thiết bị mạng chính	Có	

1.2. Kiểm soát truy cập từ bên ngoài mạng

ST T	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 Generic Firewall 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 Generic Firewall 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 Generic Firewall và ngắt phiên kết nối VPN khi người dùng không thao tác sử dụng trong 1 khoảng thời gian

1.3 Kiểm soát truy cập từ bên trong mạng

ST T	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 Generic Firewall

1.4. Nhật ký hệ thống

Yêu cầu	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
Thiết bị		
Router outside/	+	+
SWDMZ/Microtik	+	+
SWSF/ Cisco3650	+	+
SW/Cisco2960	+	+
WAF/WAF v2secure	+	+

1.5. Phòng chống xâm nhập

ST T	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 Generic Firewall có tích hợp chức năng IPS để bảo vệ các vùng mạng trong hệ thống

2	Định kỳ cập nhật CSDL dấu hiệu phát hiện tấn công mạng	Đáp ứng	Thực hiện định kỳ cập nhật CSDL dấu hiệu phát hiện tấn công mạng trên Tường lửa Generic Firewall.
---	--	---------	---

1.6. Bảo vệ thiết bị hệ thống

Yêu cầu	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
Thiết bị			
Router Mikrotik	+	+	+
Firewall (Mikrotik có tính năng tường lửa)	+	+	+
SWDMZ/Cisco2960	+	+	+
SW Cisco3650	+	+	+
SWSF/ Cisco2960	+	+	+
SW/Cisco2960	+	+	+
WAF/WAF v2secure	+	+	+

2. Bảo đảm an toàn máy chủ

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	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;
----------------	--	---	---

Máy chủ		hoặc vô hiệu hóa	Thiết lập thời gian mật khẩu hợp lệ
Web Server (máy ảo, vật lý)/Cài đặt Web-App/Vùng DMZ/ Window Server 2014, 2016, 2019/ Ubuntu 18.04	+	+	+
Database Server (máy ảo)/Cài đặt SQL server 2014, MySql Server, IBM Domino Server, PostgreSQL Server, Mysql mariadb Server 10, Oracle server 11gR2/Vùng máy chủ nội bộ/ Window Server 2019, Linux	+	+	+

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		
Web Server (máy ảo, vật lý)/Cài đặt Web-App/Vùng DMZ/ Window Server 2014, 2016, 2019/ Ubuntu 18.04	+	+
Database Server (máy ảo)/Cài đặt SQL server 2014, MySql	+	+

Server, IBM Domino Server, PostgreSQL Server, Mysql mariadb Server 10, Oracle server 11gR2/Vùng máy chủ nội bộ/ Window Server 2019 và Linux		
---	--	--

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			
Web Server (máy ảo, vật lý)/Cài đặt Web-App/Vùng DMZ/ Window Server 2014, 2016, 2019/ Ubuntu 18.04	+	+	+
Database Server (máy ảo)/Cài đặt SQL server 2014, MySql Server, IBM Domino Server, PostgreSQL Server, Mysql mariadb Server 10, Oracle server 11gR2/Vùng máy chủ nội bộ/ Window Server 2019 và Linux	+	+	+

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				
Web Server (máy ảo, vật lý)/Cài đặt Web-App/Vùng DMZ/ Window Server 2014, 2016, 2019/ Ubuntu 18.04	+	+	+	+
Database Server (máy ảo)/Cài đặt SQL server 2014, MySql Server, IBM Domino Server, PostgreSQL Server, Mysql mariadb Server 10, Oracle server 11gR2/Vùng máy chủ nội bộ/ Window Server 2019 và Linux	+	+	+	+

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		
Web Server (máy ảo, vật lý)/Cài đặt Web-App/Vùng	+	+

DMZ/ Window Server 2014, 2016, 2019/ Ubuntu 18.04		
Database Server (máy ảo)/Cài đặt SQL server 2014, MySql Server, IBM Domino Server, PostgreSQL Server, Mysql mariadb Server 10, Oracle server 11gR2/Vùng máy chủ nội bộ/ Window Server 2019 và Linux	+	+

2.6. Xử lý máy chủ khi chuyển giao

ST T	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	Đáp ứng	Hiện tại chưa có phương án chuyển giao cho đơn vị khác 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

3. Bảo đảm an toàn ứng dụng

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	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
Ứng dụng				

Hệ thống quản lý và điều hành thông tin tại Bệnh viện Lao và Bệnh phổi Cà Mau	+	+	+	+
---	---	---	---	---

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	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa
Ứng dụng			
Hệ thống quản lý và điều hành thông tin tại Bệnh viện Lao và Bệnh phổi Cà Mau	+	+	+

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 quản lý và điều hành thông tin tại Bệnh viện Lao và Bệnh phổi Cà Mau	+	+
---	---	---

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 thống quản lý và điều hành thông tin tại Bệnh viện Lao và Bệnh phổi Cà Mau	+

4. Bảo đảm an toàn dữ liệu

4.1 Bảo mật dữ liệu

ST T	Yêu cầu	P/A	Ghi chú/Mô tả
1	Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ	Có	Dữ liệu được nén và được lưu trữ mã hóa sử dụng EAS 256

4.3 Sao lưu dự phòng

ST T	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, CSDL; 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, CSDL; dữ liệu, thông tin nghiệp vụ trên ổ cứng di động