|  |
| --- |
| SỞ Y TẾ TỈNH KON TUM  **BỆNH VIỆN TÂM THẦN**  **E:\THANG_CNTT\LOGO\zyro-image.png**  **HỒ SƠ ĐỀ XUẤT CẤP ĐỘ**  **HỆ THỐNG THÔNG TIN CỦA BỆNH VIỆN TÂM THẦN**  **Kon Tum - 2024** |

**MỤC LỤC**

[THUẬT NGỮ, TỪ VIẾT TẮT 1](#_Toc116482074)

[DANH MỤC CÁC BẢNG 1](#_Toc116482075)

[DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ 1](#_Toc116482076)

[PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN 1](#_Toc116482077)

[1. Thông tin Chủ quản hệ thống thông tin 1](#_Toc116482078)

[2. Thông tin Đơn vị vận hành 1](#_Toc116482079)

[3. Mô tả phạm vi, quy mô của hệ thống 1](#_Toc116482080)

[4. Mô tả cấu trúc của hệ thống 1](#_Toc116482081)

[**4.1. Mô hình logic tổng thể** 1](#_Toc116482082)

[**4.2. Mô hình kết nối vật lý** 1](#_Toc116482083)

[**4.3. Danh mục thiết bị sử dụng trong hệ thống** 1](#_Toc116482084)

[**4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống** 1](#_Toc116482085)

[**4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống** 1](#_Toc116482086)

[PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT 1](#_Toc116482087)

[1. Danh mục hệ thống thông tin và cấp độ đề xuất 1](#_Toc116482088)

[2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin 1](#_Toc116482089)

[PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM 1](#_Toc116482090)

[AN TOÀN HỆ THỐNG THÔNG TIN 1](#_Toc116482091)

[PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 1 1](#_Toc116482092)

[**5.1.1. Thiết lập chính sách an toàn thông tin** 1](#_Toc116482093)

[**5.1.2. Tổ chức bảo đảm an toàn thông tin** 1](#_Toc116482094)

[**5.1.3. Bảo đảm nguồn nhân lực** 1](#_Toc116482095)

[**5.1.4. Quản lý thiết kế, xây dựng hệ thống thông tin** 1](#_Toc116482096)

[**5.1.5. Quản lý vận hành hệ thống thông tin** 1](#_Toc116482097)

[**5.1.6. Phương án Quản lý rủi ro an toàn thông tin** 1](#_Toc116482098)

[**5.1.7. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin** 1](#_Toc116482099)

[PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG CẤP ĐỘ 1 1](#_Toc116482100)

[**5.2.1. Bảo đảm an toàn mạng** 1](#_Toc116482101)

[**5.2.2. Bảo đảm an toàn máy chủ** **Error! Bookmark not defined.**](#_Toc116482102)

[**5.2.3. Bảo đảm an toàn ứng dụng** 1](#_Toc116482103)

[**5.2.4. Bảo đảm an toàn dữ liệu** 1](#_Toc116482104)

# THUẬT NGỮ, TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **Từ viết tắt** | **Nghĩa đầy đủ** |
|  | CNTT | Công nghệ thông tin |
|  | CSDL | Cơ sở dữ liệu |
|  | LAN | Mạng nội bộ |
|  | VPN | Vitural Private Network |
|  | DNS | Domain Name Server |
|  | ATTT | An toàn thông tin |

**DANH MỤC CÁC BẢNG**

[Bảng 1. Danh mục thiết bị sử dụng trong hệ thống 1](#_Toc67302049)

[Bảng 2. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống **Error! Bookmark not defined.**](#_Toc67302050)

[Bảng 3. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống 1](#_Toc67302051)

**DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ**

[Hình 1. Cấu trúc logic của hệ thống 1](#_Toc67302056)

[Hình 2. Kết nối vật lý của hệ thống 1](#_Toc67302057)

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

**1. Thông tin Chủ quản hệ thống thông tin**

**- Tên Tổ chức: Bệnh viện Tâm thần tỉnh Kon Tum.**

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 196/QĐ-SYT ngày 11/4/2023 của Sở Y tế tỉnh Kon Tum về việc ban hành Quy chế tổ chức và hoạt động của Bệnh viện Tâm thần trực thuộc Sở Y tế tỉnh Kon Tum

- Người đại diện: Đinh Văn Khuê, Chức vụ: Giám đốc Bệnh viện.

- Địa chỉ: 138 Bắc Kạn, Phường Thắng Lợi, TP.Kon Tum, Kon Tum.

- Thông tin liên hệ:

+ Số điện thoại: 0905225477

+ Thư điện tử: dinhvankhue@gmail.com

**2. Thông tin đơn vị vận hành.**

**- Tên đơn vị vận hành: Phòng Tổ chức –Hành chính – Kế hoạch –Tài chính**

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 10/QĐ-BVTT ngày 24/7/2023 của Bệnh viện Tâm thần về việc ban hành Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của phòng Tổ chức -Hành chính –Kế hoạch -Tài chính thuộc Bệnh viện Tâm thần tỉnh Kon Tum.

- Người đại diện: Ông Trần Văn Đại, Chức vụ: Phó trưởng phòng

- Địa chỉ: 138 Bắc Kạn, Phường Thắng Lợi, TP.Kon Tum, Kon Tum.

- Thông tin liên hệ:

+ Số điện thoại: 0976129099

+ Thư điện tử: daibvttkt@gmail.com

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

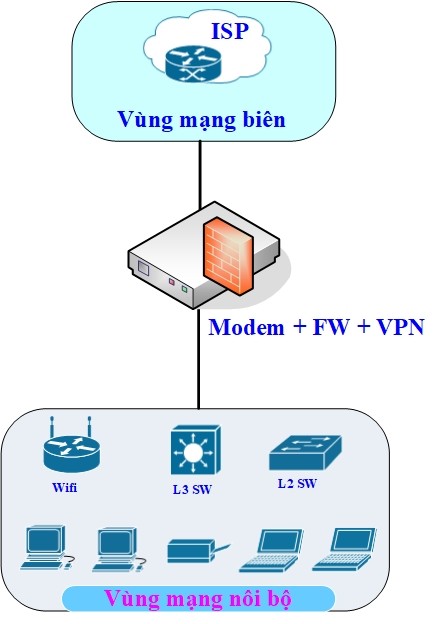
- Phạm vi, quy mô của Hệ thống mạng LAN: Hệ thống thông tin của Bệnh viện Tâm thần được thiết lập để phục vụ công tác ứng dụng công nghệ thông tin như Khám chữa bệnh, chuyển đổi số, công tác chỉ đạo điều hành, hoạt động nội bộ của Bệnh viện.

- Đối tượng phục vụ của hệ thống: viên chức, người lao động và người dân đến khám, chữa bệnh tại Bệnh viện.

**4. Mô tả cấu trúc của hệ thống**

***4.1. Mô hình logic tổng thể***

a) Sơ đồ hiện trạng



b) Sơ đồ quy hoạch mới đáp ứng yêu cầu an toàn



Hình 1. Cấu trúc logic của hệ thống

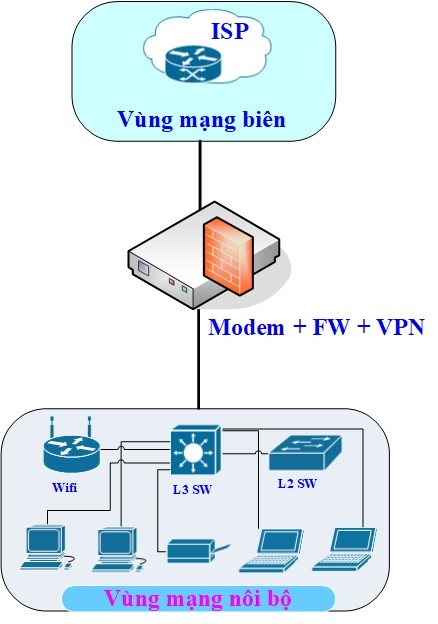
Các vùng mạng được thiết kế như sau:

+ 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***

a) Sơ đồ hiện trạng

****

b) Sơ đồ quy hoạch lại để đáp ứng yêu cầu an toàn



Hình 2. Kết nối vật lý của hệ thống

***4.3. Danh mục thiết bị sử dụng trong hệ thống***

a) Thiết bị hiện có

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên thiết bị/**  **Chủng loại** | **Vị trí triển khai** | **Mục đích sử dụng** |
| 1 | Modem/VNPT | Vùng mạng biên | Kết nối và định tuyến động với các Router của ISP. |
| 2 | Wifi/TPlink | 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

b) Thiết bị cần trang bị để đáp ứng yêu cầu an toàn

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên thiết bị/**  **Chủng loại** | **Vị trí triển khai** | **Mục đích sử dụng** |
| 1 | Firewall01/Fortigate | 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. |

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

(Hệ thống không có ứng dụng/dịch vụ trực tuyến)

***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 | 192.168.1.0/24 | 202.191.z.y |

Bảng 2. 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 Bệnh viện Tâm thần 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 thông tin phục vụ nội bộ cơ quan tại Bệnh viện (Mạng nội bộ LAN) | 1 | Điều 7/NĐ85 |
| 2 | Trang Thông tin điện tử (Hệ thống Cổng thông tin nội bộ) | 1 | Điều 7/NĐ85 |

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

# *2.1. Hệ thống mạng LAN tại Bệnh viện Tâm thần*

Hệ thống mạng LAN chỉ xử lý thông tin công khai và phục vụ hoạt động nội bộ cho cán bộ của Bệnh viện. Căn cứ theo quy định tại Điều 7/NĐ85, hệ thống này được đề xuất cấp độ 1.

***2.2. Hệ thống trang Thông tin điện tử***

Hệ thống Cổng Thông tin điện tử của Bệnh viện phục vụ hoạt động nội bộ của đơn vị và chỉ xử lý thông tin công cộng. 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**

**I. Thuyết minh phương án về quản lý**

**1. Thiết lập chính sách an toàn thông tin**

- Đảm bảo an toàn thông tin trong toàn hệ thống mạng LAN tại Bệnh viện; Cổng Thông tin điện tử Bệnh viện; xử lý văn bản điện tử đảm bảo an toàn, bí mật Nhà nước.

- Chính sách bảo đảm an toàn thông tin trong hoạt động nội bộ tại Bệnh viện phải có các quy định và ràng buộc cụ thể mà mỗi viên chức, người lao động trong cơ quan phải tuân thủ khi tham gia vào hệ thống khai thác tài nguyên thông tin; phù hợp tình hình thực tế tại Bệnh viện Tâm thần.

**2. Tổ chức bảo đảm an toàn thông tin**

Mục tiêu là đưa ra mô hình, cách thức tổ chức cho khoa, phòng để đảm bảo việc xây dựng, triển khai và thực hiện tuân thủ các chính sách về an toàn thông tin được xây dựng, triển khai tại Bệnh viện Tâm thần; Duy trì đảm bảo an toàn thông tin trong hoạt động nội bộ; cung cấp thông tin phục vụ người dân tốt hơn.

# *2.1. Đơn vị chủ trì*

- Phòng Tổ chức – Hành chính – Kế hoạch – Tài chính, Bệnh viện Tâm thần chủ trì phối hợp với các khoa, phòng liên quan thực hiện tốt quy chế đảm bảo an toàn thông tin trong hệ thống mạng nội bộ LAN.

- Là đầu mối tổ chức thực hiện, tiếp nhận và xử lý các sự cố cơ bản về an toàn thông tin trong hoạt động nội bộ cơ quan.

- Phối hợp với Sở Y tế và các đơn vị liên quan kịp thời xử lý những sự cố mất an toàn thông tin ngoài khả năng xử lý của phòng.

# *2.2. Người sử dụng*

- Người sử dụng có trách nhiệm quản lý tài khoản đối với các phần mềm; thực hiện nghiêm các quy định về đảm bảo an toàn thông tin trong hệ thống mạng LAN tại Bệnh viện.

- Tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

# *2.3. Cán bộ quản lý và vận hành hệ thống*

- Xây dựng quy chế đảm bảo an toàn thông tin trong toàn hệ thống.

- Theo dõi viên chức nghỉ việc, thay đổi vị trí công tác để hủy bỏ, thay đổi tài khoản đăng nhập các phần mềm cho phù hợp.

- Tham gia các chương trình đào tạo về an toàn thông tin do các sở, ban, ngành cấp tỉnh tổ chức.

# *2.4. Quản lý sự cố an toàn thông tin*

Viên chức Công nghệ thông tin có trách nhiệm:

- Phối hợp với Sở Y tế và các sở, ban, ngành liên quan phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng.

- Phối hợp xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/NĐ-CP.

- Phối hợp triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/NĐ-CP.

- Phối hợp với Sở Y tế và các sở, ban, ngành cấp tỉnh hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin.

# *2.5. Quản lý an toàn người sử dụng*

Người sử dụng phải thông tin, báo cáo kịp thời cho viên chức Công nghệ thông tin của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

**3. Bảo đảm nguồn nhân lực**

-Viên chức được tuyển dụng vào vị trí làm về an toàn thông tin tại Bệnh viện có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng.

- Mỗi viên chức và người lao động trong Bệnh viện phải nắm rõ vai trò, trách nhiệm của mình khi tham gia vận hành, khai thức, xử lý thông tin trên môi trường mạng trong hệ thống mạng LAN tại Bệnh viện; Nhằm giảm thiểu các rủi ro về việc lộ lọt thông tin, bí mật nhà nước; rà soát, tổng hợp danh sách các cá nhân đã nghỉ việc hoặc thuyên chuyển công tác để loại ra khỏi hệ thống.

**4. Quản lý thiết kế, xây dựng hệ thống**

Khi thiết kế, xây dựng hệ thống phải đảm bảo các nguyên tắc sau:

- Phân vùng mạng để đảm bảo kiểm soát truy cập hệ thống

- Thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các hiểm họa và duy trì an toàn cho các hệ thống, ứng dụng sử dụng mạng:

+ Có sơ đồ logic và vật lý về hệ thống mạng

+ Sử dụng tường lửa, thiết bị phát hiện và ngăn chặn xâm nhập và các trang thiết bị khác đảm bảo an toàn thông tin.

**5. Quản lý vận hành hệ thống**

***5.1. Đối với thiết bị CNTT***

- Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống Công nghệ thông tin trong mạng LAN.

- Cần trang bị (Switch) trong cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng.

- Cần trang bị Tường lửa (firewall) nhằm hạn chế việc truy cập trái phép từ bên ngoài.

***5.2. Đối với trang Thông tin điện tử đơn vị***

***\* Yêu cầu đơn vị triển khai:***

- Là đơn vị được thuê dịch vụ hosting đặt Cổng Thông tin điện tử Bệnh viện thực hiện quản lý toàn bộ các phiên bản của mã nguồn, tổ chức mô hình trang web hợp lý, tránh nguy cơ tấn công; Phải cài đặt các hệ thống phòng vệ như tường lửa, thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web.

- Hàng tháng đơn vị triển khai thực hiện việc Backup toàn bộ nội dung trang web, gồm mã nguồn, cơ sở dữ liệu... để bảo đảm khi có sự cố có thể khắc phục lại trong thời gian nhanh nhất.

***\* Đối với quản trị website:***

- Quản trị website Cổng Thông tin điện tử Bệnh viện thực hiện bảo mật tài khoản quản trị, thường xuyên đổi mật khẩu đủ mạnh (Ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt); tạo tài khoản và phân công quyền đăng tải một số nội dung cho các thành viên được phân công.

- Ban biên tập Cổng Thông tin điện tử Bệnh viện thực hiện phân công nhiệm vụ cụ thể cho từng thành viên, mỗi thành viên được giao nhiệm vụ phải chịu hoàn toàn trách nhiệm trước Trưởng Ban và trước Pháp luật về những nội dung được phân công phụ trách; thực hiện đăng tải đầy đủ các nội dung theo quy định tại Nghị định số 42/2022/NĐ-CP.

***5.3. Quy định về quản lý phòng chống phần mềm độc hại***

- Tất cả các máy trạm, máy chủ trong cơ quan phải được cài đặt phần mềm diệt virus bản quyền (hoặc của hệ điều hành), hàng năm phải được bảo trì, cài đặt phần mềm vá lỗi thường xuyên.

- Khi gửi văn bản điện tử gửi qua hệ thống thư điện tử hoặc xử lý công việc trên phần mềm Quản lý văn bản, phần mềm theo dõi nhiệm vụ phải có định dạng theo Danh mục tiêu chuẩn kỹ thuật về ứng dụng CNTT trong cơ quan nhà nước như: (.txt), (.doc), (.odt), (.pdf) và các định dạng khác theo quy định, không được gửi các file thực thi (.com), (.bat), (.exe)…

- Các cán bộ, công chức, viên chức và người lao động trong cơ quan không được tự ý cài đặt hoặc gỡ bỏ phần mềm diệt vius trên máy trạm.

- Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,…), người sử dụng phải báo ngay cho Tổ CNTT để xử lý.

***5.4. Phòng chống xâm nhập***

Sử dụng tường lửa trong hệ thống để ngăn chặn các truy cập trái phép từ bên ngoài tác động vào hệ thống.

**II. Thuyết minh phương án về kỹ thuật**

**1. Bảo đảm an toàn mạng**

***1.1. Thiết kế hệ thống***

- Hệ thống mạng LAN tại Bệnh viện chưa được đầu tư thiết kế hệ thống.

***1.2. Kiểm soát truy cập từ bên ngoài mạng***

- Hệ thống mạng LAN tại Bệnh viện chưa được đầu tư thiết bị tường lửa nhằm hạn chế sự truy cập trái phép từ bên ngoài.

***1.3. Nhật ký hệ thống***

Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: Thông tin truy cập ứng dụng; Thông tin xem văn bản đi, đến; Thông tin các lỗi phát sinh trong quá trình xử lý công việc; Thông tin thay đổi cấu hình ứng dụng.

***1.4. Phòng chống xâm nhập***

- Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật, tự động rò quét trên các máy trạm trong hệ thống.

- Hàng năm thực hiện bảo trì, vá lỗi, cài phần mềm diệt virus có bản quyền trên tất cả các máy trạm.

***1.5. Bảo vệ thiết bị hệ thống***

**2. Bảo đảm an toàn ứng dụng**

***2.1. Xác thực***

- Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập vào 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 người dùng.

***2.2. Kiểm soát truy cập***

- Thiết bị tường lửa chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập vào hệ thống.

- Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi sử dụng các phần mềm dùng chung khi không nhận được yêu cầu từ người dùng.

- Tắt các chức năng remote desktop tại các máy trạm trong hệ thống để chặn các kết nối từ xa.

***2.3. Nhật ký hệ thống***

Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: Thông tin truy cập ứng dụng; Thông tin xem văn bản đi, đến; Thông tin các lỗi phát sinh trong quá trình xử lý công việc; Thông tin thay đổi cấu hình ứng dụng.

**3. Bảo đảm an toàn dữ liệu**

***3.1. Nguyên vẹn dữ liệu***

Xây dựng phương án bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; giám sát, cảnh báo khi có thay đổi hoặc phát hiện, ngăn chặn các tác động truy nhập, gửi, nhận dữ liệu trái phép; Thực hiện ký số cá nhân từ chuyên viên để xác thực và bảo mật thông tin, dữ liệu, đặc biệt trong trường hợp cần bảo đảm chống từ chối nguồn gốc dữ liệu.

- Bố trí máy tính riêng không kết nối mạng, đặt mật khẩu, mã hóa dữ liệu và các biện pháp bảo mật khác bảo đảm an toàn thông tin để soạn thảo, lưu trữ dữ liệu, thông tin và tài liệu quan trọng ở các mức độ mật, tối mật, tuyệt mật.

***3.2. Bảo mật dữ liệu***

- Thực hiện mã hóa dữ liệu đối với tất cả văn bản ban hành của (Đơn vị).

- Thực hiện cài đặt mật khẩu đủ mạnh đối với tài khoản đăng nhập vào hệ thống các phần mềm và máy tính cá nhân.

- Cài đặt phần mềm virus có bản quyền và thường xuyên quét virus.

***3.3. Sao lưu dự phòng***

- Mục đích của sao lưu dự phòng là tạo một bản dữ liệu khác có thể được phục hồi trong trường hợp xảy ra với bản chính với bất kỳ nguyên nhân nào; có thể là lỗi phần cứng hoặc phần mềm, do hỏng hoặc do con người gây ra, chẳng hạn như virus tấn công (vi-rút hoặc phần mềm độc hại) hoặc xóa nhầm dữ liệu ngẫu nhiên. Bản sao lưu cho phép dữ liệu được khôi phục từ thời điểm trước đó để giúp cán bộ, công chức khôi phục từ những việc bất khả kháng trên.

- Thực hiện lưu trữ an toàn theo cách: Sao lưu dữ liệu điện tử và sao lưu dữ liệu dự phòng trên thiết bị di động hoặc ổ đĩa máy tính (nén và đặt mật khẩu)...

**III. Thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống**

|  |  |  |  |
| --- | --- | --- | --- |
| **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 |
|  | Hệ thống Cổng/trang Thông tin điện tử Bệnh viện | 1 | Phụ lục III |

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

**1. Thiết lập chính sách an toàn thông tin**

***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** | **Chưa đáp ứng** |

***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** | **Chưa đáp ứng** |

***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** | **Chưa đáp ứng** |

**2. Tổ chức bảo đảm an toàn thông tin**

***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** |

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

|  |  |
| --- | --- |
| **Yêu cầu**  **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** |
| **Yêu cầu**  **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** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  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) Sở Thông tin và Truyền thông tỉnh Kon tum**  - Người liên hệ: Hoàng  + Số điện thoại: 0982133377  + Email:  **b) 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 |

**3. Bảo đảm nguồn nhân lực**

***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** |

***3.2. Trong quá trình làm việc***

|  |  |
| --- | --- |
| **Yêu cầu**  **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** |
| **Yêu cầu**  **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** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  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. |

***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** | **Chưa đáp ứng** |

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

***4.1. Thiết kế an toàn hệ thống thông tin***

|  |  |
| --- | --- |
| **Yêu cầu**  **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** | **Chưa đáp ứng** |
| **Phương án** | 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**  **4.1.b** | Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin. |
| **Hiện trạng** | **Chưa đáp ứng** |
| **Phương án** | 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. |

***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** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  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 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. Quản lý vận hành hệ thống thông tin**

***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** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  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. |

***5.2. Quản lý an toàn ứng dụng***

|  |  |
| --- | --- |
| **Yêu cầu** | Xây dựng và thực thi chính sách, quy trình quản lý, vận hành hoạt động bình thường của ứng dụng. |
| **Hiện trạng** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  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. |

***5.3. 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** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  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. |

**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** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quy định về Quản lý rủi ro an toàn thông tin:  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:  a. 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. |

**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** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:  1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành 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.  2. 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. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng. |

**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 viên chức và người lao động tại Bệnh viện Tâm thần. 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:

**1. Bảo đảm an toàn mạng**

***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 | Chưa có | Thiết lập cấu hình VPN trên tường lửa Firewall01 cho phép người vận hành, người sử dụng quản lý truy cập, quản trị hệ thống từ xa an toàn. |
| 2 | Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập | Chưa có | Thiết lập cấu hình chức năng IDS/IPS trên các luật/các giao diện của tường lửa Firewall 01 để quản lý truy cập và phòng, chống xâm nhập giữa vùng mạng LAN và mạng biên. |
| 3 | Phương án phòng chống mã độc cho máy chủ và máy trạm |  | Cài đặt phần mềm phóng, chống mã độc cho toàn bộ máy trạm có trong hệ thống sử dụng giải pháp AV (hoặc EDR) của hãng BKAV |

***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 | Chưa có | Cấu hình trên Firewall01 chỉ cho phép người quản trị, người sử dụng truy cập vào các tài nguyên hệ thống thông qua kết nối VPN. |

***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/VNPT | + |
| Firewall01/Fortigate | + |
| Switch L2/Cisco | + |
| Wifi/TPLink | + |

***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 | Chưa có | N/A |
| 2 | Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng | Chưa có | Firewall01 có bản quyền cho chức năng IDS/IPS. Chức năng IDS/IPS trên Firewall01 được cấu hình để tự động cập nhật dấu hiệu phát hiện xâm nhập tự động hàng ngày. |

***1.5. Bảo vệ thiết bị hệ thống***

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | 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. |
| **Thiết bị** |
| Modem/VNPT | + | + |
| Firewall01/Fortigate | + | + |
| Switch L2/Cisco | + | + |
| Wifi/TPLink | + | + |

**2. Đảm an toàn ứng dụng**

***2.1. 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** |
| NA | NA | NA | NA |

***2.2. 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** |
| NA | NA | NA |

***2.3. 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** |
| NA | NA |

**3. Bảo đảm an toàn dữ liệu**

***3.1. 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 trên thiết bị lưu trữ USB, DVD… |

**PHỤ LỤC III. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG TRANG THÔNG TIN ĐIỆN TỬ TRUNG TÂM Y TẾ**

**ĐỀ XUẤT CẤP ĐỘ 1**

**1. Bảo đảm an toàn máy chủ**

Máy chủ cung cấp dịch vụ Hosting được đặt tại Viễn thông Kon Tum. Yêu cầu Viễn thông Kon Tum thực hiện các nội dung sau:

***1.1. Xác thực***

- 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.

***1.2. Kiểm soát truy cập***

Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập vào hệ thống.

***1.3. Nhật ký hệ thống***

- Cài đặt Web-App để thiết lập chức năng ghi nhật ký hệ thống trên các máy chủ.

- Thực hiện đồng bộ thời gian giữa máy chủ với thời gian hiện tại theo đúng múi giờ của Việt Nam.

***1.4. Thực hiện các biện pháp phòng, chống xâm nhập***

- 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.

***1.5. Phòng chống các phần mềm độc hại***

Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật trên máy chủ.

***2. Bảo đảm an toàn ứng dụng:***

***2.1. Xác thực***

Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập vào hệ thống và đảm bảo an toàn mật khẩu người sử dụng.

***2.2. Kiểm soát truy cập***

Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập vào hệ thống và thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng.

***3.3. Nhật ký hệ thống***

Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: Thông tin truy cập ứng dụng; Thông tin ứng dụng khi đăng nhập vào hệ thống.