SỞ GIÁO DỤC VÀ ĐÀO TẠO QUẢNG NGÃI

TRƯỜNG THPT MINH LONG

HỒ SƠ

ĐỀ XUẤT CẤP ĐỘ
CHO HỆ THỐNG THÔNG TIN MẠNG NỘI BỘ
CỦA TRƯỜNG THPT MINH LONG

Minh Long – 2024

MỤC LỤC

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
1.	CNTT	Công nghệ thông tin
2.	CSDL	Cơ sở dữ liệu
3.	LAN	Mạng nội bộ

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

1. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: Sở Giáo dục và Đào tạo Quảng Ngãi

- Người đại diện: : Ông Nguyễn Ngọc Thái, Chức vụ: Giám đốc Sở

- Địa chỉ chủ sở đơn vị: Số 58 Hùng Vương, Thành phố Quảng Ngãi, Tỉnh Quảng Ngãi.

- Thông tin liên hệ: 0255.3824164; Email: vanphongso@quangngai.edu.vn

2. Thông tin Đơn vị vận hành

- Tên Đơn vị vận hành: Trường THPT Minh Long

- Người đại diện: : Ông Lê Ngọc Đức, Chức vụ: Hiệu Trưởng.

- Địa chỉ: Thôn Mai Lãnh Hữu, xã Long Mai – huyện Minh Long - tỉnh Quảng Ngãi.

- Thông tin liên hệ: 02553866195. Email: c3minhlong@quangngai.edu.vn

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống thông tin mạng nội bộ (LAN) Trường THPT Minh Long được thiết lập để phục vụ hoạt động nội bộ của đơn vị và công tác chỉ đạo điều hành trong phạm vi của trường.

- Đối tượng phục vụ của hệ thống: Cán bộ, giáo viên, nhân viên và người lao động; học sinh của trường. Các cơ quan, ban, ngành có liên quan.

- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi Hệ thống:

+ Trang thông tin điện tử

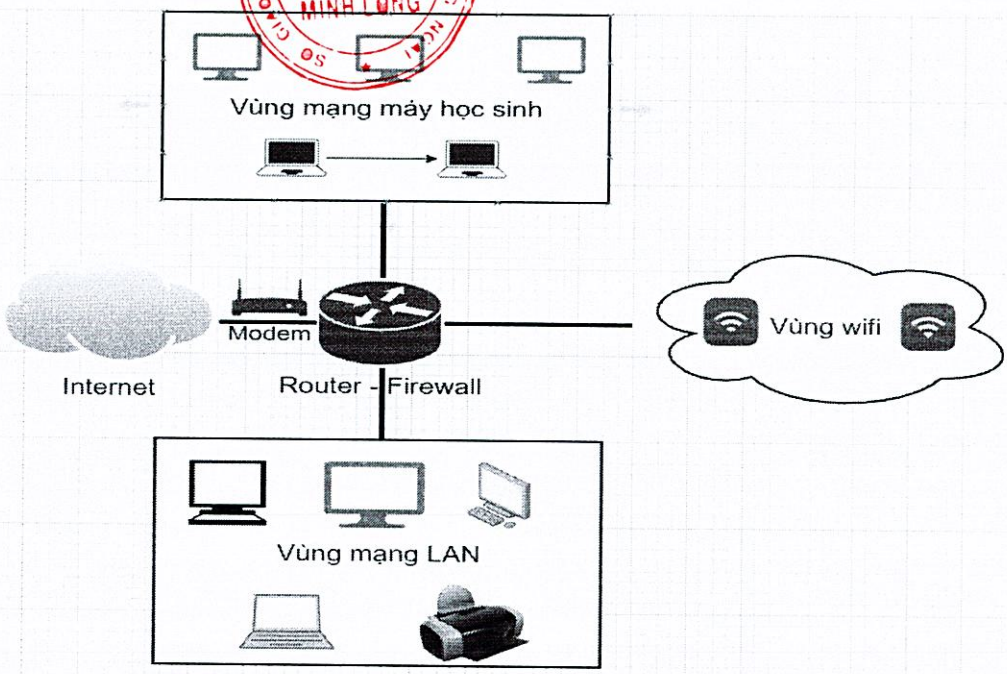
+ Hệ thống gửi, nhận văn bản điện tử

+ Phần mềm quản lý chuyên ngành

+ Hệ thống cổng thông tin nội bộ.

4. Mô tả cấu trúc của hệ thống

4.1. Sơ đồ logic tổng thể



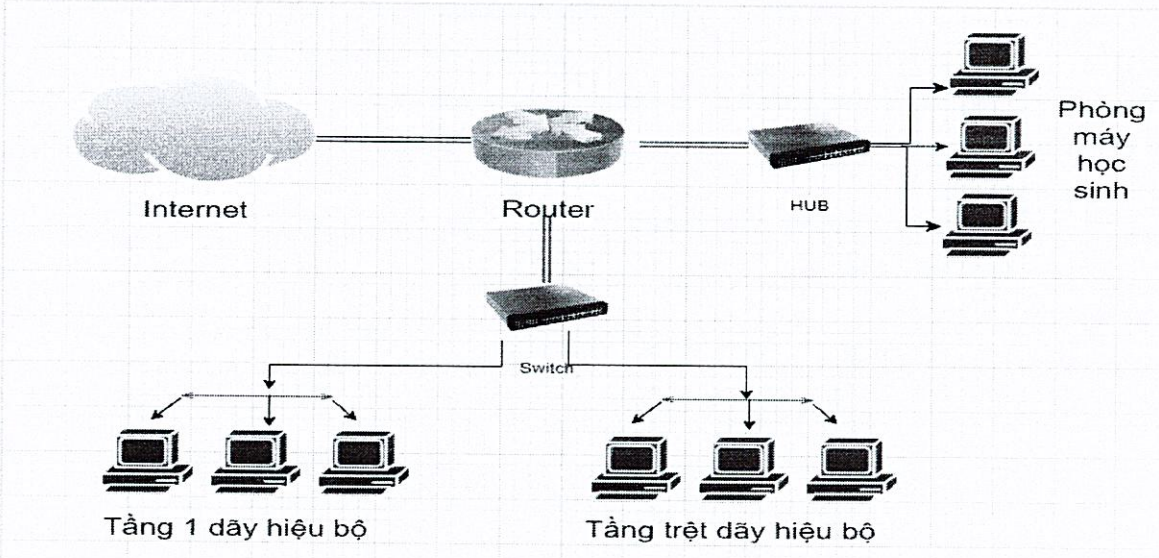
Hình 1: Sơ đồ logic tổng thể hệ thống mạng trường THPT Minh Long

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. Sơ đồ kết nối vật lý



Hình 2: Sơ đồ kết nối vật lý tổng thể hệ thống mạng trường THPT Minh Long

4.3. Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Modem VNPT GPON iGate GW240	Vùng mạng biên	Kết nối và định tuyến động với các Router của ISP
2	TP-LINK TL-SE106D	Vùng mạng nội bộ	Thiết bị thu sóng đưa tín hiệu mạng chuyên dùng và mạng công cộng xuống Swtich
3	TP-Link 24 Port Gigabit Switch	Vùng mạng nội bộ	Bộ chia tín hiệu để bàn nhỏ gọn với 24 cổng, cung cấp Internet cho người dùng nội bộ
4	Wifi	Mạng wifi	Thiết bị cung cấp kết nối internet không dây cho vùng mạng nội bộ
5	Totolink N600R	Vùng mạng nội bộ	Bộ mở rộng thu sóng đưa tín hiệu mạng chuyên dùng xuống Switch
6	Đầu ghi KBVISION	Vùng mạng nội bộ	Lưu trữ dữ liệu, backup dữ liệu của hệ thống từ các camera giám sát

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

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

STT	Tên dịch vụ	Máy chủ/Ứng dụng cài đăt/Vùng mạng/HĐH	Mục đích sử dụng
1	Cổng thông tin nội bộ	Văn Phòng/ Cài đặt app/ Vùng mạng nội bộ/ HĐH Window Pro 10	Cung cấp thông tin công khai cho người sử dụng nội bộ.
2	Phần mềm eOffice	Văn Phòng/ Cài đặt app /Vùng mạng nội bộ/ HĐH Windows 10 Pro	Quản lý và điều hành văn

			bản eOffice
3	Hệ thống mạng nội bộ - LAN của đơn vị	Router, Camera,..	Cung cấp đường truyền; kết nối, liên thông với các hệ thống liên quan qua môi trường Internet

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

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

STT	Vùng mạng	IP Private	IP Public
1	Vùng mạng LAN	192.168.1.x/24	Auto
2	Vùng mạng máy học sinh	192.168.10.x/24	Auto
3	Vùng mạng Wifi	192.168.11.x/24	Auto

- Quy hoạch địa chỉ IP động để hạn chế trùng địa chỉ IP.

- Quy hoạch lớp IP cho hệ thống Wifi riêng để không ảnh hưởng đến lớp IP trong hệ thống.

4.6. Thuyết minh chính sách, cơ chế bảo mật, cơ chế truy cập của các lớp mạng và giữa các lớp mạng trong hệ thống

Trường THPT Minh Long hiện không có hệ thống Server và tường lửa nên về cơ bản hệ thống không được bảo vệ. Hệ thống mạng tại đơn vị cụ thể như sau:

1	Vùng mạng nội bộ LAN	- Được bố trí phân chia thành 01 dãy IP để thuận tiện trong công tác quản lý hệ thống. - Cho phép truy cập Internet với cơ chế lọc an toàn trên thiết bị Modem. - Cho phép sử dụng và khai thác dữ liệu dùng chung của đơn vị cơ chế bảo mật bằng phân quyền tài khoản.
2	Vùng máy học sinh	- Được thiết lập chỉ cho phép truy cập Internet và chia sẻ dữ liệu nội bộ trong vùng mạng. - Không được truy cập vào vùng nội bộ và các vùng mạng khác trên hệ thống

3	Vùng Wifi	- Được thiết lập chỉ cho phép truy cập Internet - Không được truy cập vào vùng nội bộ và các vùng mạng khác trên hệ thống

PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

Căn cứ Điều 8 Nghị định số 85/2016/NĐ-CP ngày 01/7/2017 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ. Hệ thống thông tin Trường THPT Minh Long là hệ thống cơ sở hạ tầng thông tin thuê dịch vụ và hệ thống mạng nội bộ.

Danh mục hệ thống thông tin và cấp độ đề xuất tương ứng:

STT	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống mạng LAN phục vụ công tác chỉ đạo điều hành, hoạt động nội bộ cơ quan tại trường THPT Số 2 Nghĩa Hành.	1	Điều 7, Nghị định 85/2016/NĐ-CP

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

Hệ thống thông tin mạng nội bộ (LAN) Trường THPT Minh Long:

Hệ thống chỉ xử lý thông tin công khai và phục vụ hoạt động nội bộ cho cán bộ, viên chức và người lao động của Trường THPT Minh Long. Căn cứ theo quy định tại Khoản 3, 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

1. Thiết lập chính sách an toàn thông tin

a) Mục tiêu, nguyên tắc bảo đảm an thông tin

- Mục tiêu bảo đảm an toàn thông tin là bảo vệ thông tin, hệ thống thông tin tránh bị truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của hệ thống thông tin.

- Hoạt động an toàn thông tin mạng tại trường THPT Minh Long đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

- Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

- Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

- Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

- Bố trí kinh phí để đảm bảo an toàn hệ thống thông tin thực hiện theo thứ tự ưu tiên từ cấp độ cao xuống cấp độ thấp.

b. Trách nhiệm của cán bộ chuyên trách đảm bảo an thông tin

- Đảm bảo vận hành tốt đối với hệ thống thông tin thuộc phạm vi xử lý.

- Định kỳ kiểm tra công tác bảo đảm an toàn thông tin mạng LAN theo chỉ đạo của lãnh đạo nhà trường hoặc theo hướng dẫn của Sở Thông tin và Truyền thông.

- Ứng cứu các sự cố an toàn thông tin mạng.

- Tham mưu cho Hiệu trưởng chỉ đạo, thực hiện nghiêm túc, đảm bảo an toàn, an ninh thông tin, hướng dẫn đến viên chức và người lao động tại đơn vị về công tác bảo đảm an toàn thông tin mạng.

- Đề xuất sữa chữa, nâng cấp, thay thế trang thiết bị không phù hợp để đảm bảo an toàn thông tin trong toàn hệ thống.

c. Trách nhiệm của viên chức và người lao động trong cơ quan

- 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.

- Tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; Khai thác, sử dụng có hiệu quả các phần mềm dùng chung của Trường.

- Phối hợp với viên chức quản trị an toàn thông tin tại đơn vị trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin.

2. Tổ chức bảo đảm an toàn thông tin

- Đưa ra mô hình, cách thức tổ chức cho các phòng, cá nhân liên quan 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 Trường.

- Duy trì đảm bảo an toàn thông tin trong hoạt động nội bộ.

- Cung cấp thông tin phục vụ người dân, tổ chức, doanh nghiệp ngày càng tốt hơn.

3. Bảo đảm nguồn nhân lực

- Cán bộ, viên chức và người lao động của đơn vị đều đã qua các lớp bồi dưỡng về tin học văn phòng và có khả năng sử dụng khai thác được mạng internet cũng như ứng dụng các phần mềm phục vụ cho công việc.

- Mỗi cán bộ, viên chức và người lao động của đơn vị nhận thức rõ vai trò, trách nhiệm của mình khi tham gia vận hành, khai thác, xử lý các thông tin trên môi trường mạng trong hệ thống mạng LAN cơ quan nhằm giảm thiểu các rủi ro về việc lộ thông tin nội bộ.

- Tổng hợp danh sách các cá nhân đã nghỉ việc, nghỉ hưu hoặc thuyên chuyển công tác để loại ra khỏi hệ thống.

- Cán bộ phụ trách lĩnh vực an toàn, an ninh thông tin tại Trường phải có trình độ Đại học Công nghệ thông tin chuyên ngành, có chứng chỉ bồi dưỡng về an toàn, an ninh thông tin do Sở Thông tin và Truyền thông tổ chức.

4. Quản lý thiết kế, xây dựng hệ thống

- Thiết bị chuyển mạch (switch, router) trong cơ quan đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng.

- Thiết bị GPON iGate GW240 được tích hợp NAT, SPI Firewall (tường lửa) chống tấn công từ chối dịch vụ Dos, SYN Flooding để thiết lập các cơ chế bảo mật trên hệ thống.

5. Quản lý vận hành hệ thống

- Quản lý an toàn mạng:

+ Đảm bảo an toàn thông tin trong toàn hệ thống mạng LAN Trường THPT Minh Long nhằm thực hiện việc truy cập internet để gửi nhận, xử lý văn bản điện tử; khai thác sử dụng các phần mềm được các sở, ngành triển khai tại Trường; tìm kiếm thông tin phục vụ công tác, chỉ đạo, đều hành đảm bảo an toàn.

+ Chính sách bảo đảm an toàn thông tin trong hoạt động nội bộ cơ quan quy định và ràng buộc cụ thể mà mỗi cán bộ, viên chức và người lao động trong đơn vị phải tuân thủ khi tham gia vào hệ thống khai thác tài nguyện thông tin; phù hợp tình hình thực tế của Trường.

- Quản lý an toàn máy chủ và ứng dụng:

+ Xây dựng quy chế đảm bảo an toàn thông tin trong toàn hệ thống như: Quy trình tiếp, xử lý văn bản điện tử; Quy chế hoạt động của Cổng thông tin điện tử của Trường đảm bảo an toàn, an ninh thông tin, thông tin liên lạc hệ thống mạng đến cán bộ, viên chức và người lao động tại Trường.

+ Theo dõi, cán bộ, viên chức nghỉ hưu, 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 các cấp liên quan trong tỉnh tổ chức.

- Quản lý an toàn dữ liệu:

* Đối với viên chức quản trị hệ thống:

+ Có nhiệm vụ phân quyền truy cập cho các cán bộ, viên chức; điều chỉnh vị trí công tác cho người sử dụng (khi có sự thay đổi); xóa khỏi hệ thống các tài khoản người dùng đã về hưu, hoặc chuyển công tác, thường xuyên thay đổi mật khẩu quản trị đủ mạnh để đảm bảo an toàn, bảo mật thông tin. Mật khẩu có ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt.

+ Hướng dẫn quy trình xử lý nội bộ trên các phần mềm dùng chung của Trường cho cán bộ, viên chức tại đơn vị.

+ Tham mưu cho lãnh đạo Trường các văn bản chỉ đạo, điều hành thực hiện quản lý, tiếp nhận, xử lý, ký số, văn bản điện tử đảm bảo an toàn, hiệu quả.

+ Phối hợp với viên chức trong đơn vị rà soát kiểm tra đề xuất lãnh đạo sửa chữa, bảo trì thiết bị vi tính, cài đặt, vá lỗi phần mềm tránh nguy cơ mất an toàn, an ninh thông tin máy trạm người dùng.

* Đối với người dùng (viên chức và người lao động trong cơ quan):

+ Thường xuyên đổi mật khẩu đủ mạnh (ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt) đối với các phần mềm dùng chung của Trường.

+ Thực hiện tiếp nhận, xử lý, phát hành, quản lý và lưu trữ văn bản, hồ sơ điện tử trên các phần mềm quản lý văn bản trên môi trường mạng và ký số cá nhân, đảm bảo theo đúng quy định pháp luật hiện hành.

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

STT	Hệ thống	Cấp độ đề xuất	Nội dung thuyết minh
1	Hệ thống thông tin mạng nội bộ (LAN) của Trường THPT Minh Long	1	Phụ lục I

PHẦN IV. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÔNG TIN

1. Bảo đảm an toàn mạng

- Thường xuyên phối hợp với đơn vị cho thuê dịch vụ để vận hành hệ thống ổn định.

- Viên chức phụ trách công nghệ thông tin tại đơn vị thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn, an ninh thông tin, nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

- Thường xuyên thực hiện việc theo dõi bản ghi nhật ký các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin;

- Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin, hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

- Luôn cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu; sử dụng công để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu.

2. Bảo đảm an toàn ứng dụng

- Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của Trung tâm; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

- Nghiêm chỉnh chấp hành các quy định nội bộ về an toàn thông tin của đơn vị và các quy định khác của pháp luật.

- Thường xuyên cài đặt và cập nhật các phần mềm diệt virus... lên tất cả các máy tính cá nhân, máy tính xách tay.

- Kiểm tra và cập nhật các bản vá lỗi để sửa chữa các lỗ hổng bảo mật.

- Thiết lập chính sách lưu dự phòng dữ liệu định kỳ.

3. Bảo đảm an toàn dữ liệu

- Hệ thống mạng nội bộ của Trung tâm được thiết kế xây dựng theo mô hình nhóm (Group) cho từng phòng chức năng và cấp địa chỉ mạng cố định cho từng cá nhân cho từng máy tính của đơn vị và theo dõi nhằm mục đích quản lý hệ thống chặt chẽ, an toàn và bảo mật.

- Định kỳ lưu trữ dữ liệu vào các thiết bị lưu trữ.

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

1. Bảo đảm an toàn ứng dụng

1.1. Xác thực

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

1.2. 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 để đóng phiên kết nối khi sử dụng các phần mềm chung của Trường khi không nhận được yêu cầu từ người dùng.

1.3. Kiểm soát truy cập từ bên ngoài mạng

Hệ thống mạng nội bộ (LAN) sử dụng các tính năng từ thiết bị GPON iGate GW240 được tích hợp NAT, SPI Firewall (tường lửa) để thiết lập các cơ chế nhằm hạn chế sự truy cập từ bên ngoài.

1.4. Kiểm soát truy cập từ bên trong mạng

- Ban hành quy chế đảm bảo an toàn thông tin trong toàn hệ thống;

- Khuyến cáo người dùng không sử dụng USB để chia sẻ dữ liệu;

- Không sử dụng gmail,… để gửi, nhận văn bản trong cơ quan.

- Hằng năm các máy tính trong hệ thống mạng phải được bảo trì, vá lỗi, cài đặt phần mềm Phòng chống mã độc, nhằm phòng chống phần mềm độc hại trên môi trường mạng.

- Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ.

- Yêu cầu người sử dụng thường xuyên đổi mật khẩu và đặt mật khẩu đủ mạnh.

1.5. 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 các lỗi phát sinh trong quá trình xử lý công việc; Thông tin thay đổi cấu hình ứng dụng.

1.6. Phòng chống phần mềm độc hại

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

- Hằng năm thực hiện việc bảo trì, vá lỗi, cài phần mềm Phòng chống mã độc trên tất cả các máy trạm.

2. Bảo mật an toàn ứng dụng

- Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập vào phần mềm trên hệ thống.

- Thiết lập chế độ cảnh báo số lần đăng nhập sai trên phần mềm trong khoảng thời gian nhất định với tài khoản nhất định.

3. Bảo đảm an toàn dữ liệu

3.1. Bảo mật dữ liệu

- Thực hiện ký số cá nhân đối với tất cả văn bản của Trường.

- 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 Phòng chống mã độc và thường xuyên quét virus.

3.2. 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 một 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 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, viên chức khôi phục từ những việc bất khả trên.

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

4. Phương án đảm bảo an toàn thông tin

STT	Yêu cầu	Phương án	Ghi chú/mô tả
1	Quản lý truy cập trong hệ thống mạng nội bộ (LAN)	Có	Truy cập trong hệ thống mạng LAN tại cơ quan được sử dụng thiết bị GPON iGate

			GW240 được tích hợp NAT, SPI Firewall (tường lửa) chống tấn công từ chối dịch vụ Dos, SYN Flooding để thiết lập các cơ chế bảo mật trên hệ thống, phòng chống xâm nhập.
2	Phương án ngăn chặn phần mềm độc hại trên môi trường mạng	Có	Phần mềm chống mã độc BKAV ENDPOINT 15 Pro
3	Phương án giám sát hệ thống thông tin tập trung	Có	Thiết bị GPON iGate GW240 được tích hợp NAT, SPI Firewall (tường lửa) phòng chống xâm nhập.
4	Quản lý sao lưu dữ liệu dự phòng	Có	Sao lưu qua thiết bị ổ cứng di động.

PHỤ LỤC 2. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÔNG TIN CẤP ĐỘ 1

1. Bảo đảm an toàn mạng

- Thường xuyên phối hợp với đơn vị cho thuê dịch vụ để vận hành hệ thống ổn định;

- Viên chức phụ trách công nghệ thông tin tại đơn vị thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn, an ninh thông tin, nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

- Thường xuyên thực hiện việc theo dõi bản ghi nhật ký các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin;

- Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu nhất bảo đảm duy trì hoạt động của hệ thống thông tin; hạn chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

- Luôn cập nhật bản vá lỗi mới nhất cho hệ quản trị cơ sở dữ liệu; sử dụng công cụ để đánh giá, tìm kiếm lỗ hổng trên máy chủ cơ sở dữ liệu.

2. Bảo đảm an toàn ứng dụng

- Nghiêm chỉnh chấp hành các quy định nội bộ về an toàn thông tin của đơn vị và các quy định khác của pháp luật.

- Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của trường; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

- Thường xuyên cài đặt và cập nhật các phần mềm diệt virus... lên tất cả các máy tính cá nhân, máy tính xách tay.

- Kiểm tra và cập nhật các bản vá lỗi để sửa chữa các lỗ hổng bảo mật.

- Thiết lập chính sách lưu dự phòng dữ liệu định kỳ.

3. Bảo đảm an toàn dữ liệu

- Hệ thống mạng nội bộ của trường được thiết kế xây dựng theo mô hình nhóm (Group) cho từng phòng chức năng và cấp địa chỉ mạng cố định cho từng cá nhân cho từng máy tính của đơn vị và theo dõi nhằm mục đích quản lý hệ thống chặt chẽ, an toàn và bảo mật.

- Định kỳ sao lưu dữ liệu qua thiết bị ổ cứng di động.

NGƯỜI LẬP HỒ SƠ	THỦ TRƯỞNG ĐƠN VỊ
Trần Văn Vũ	Lê Ngọc Đức