

ỦY BAN NHÂN DÂN HUYỆN TRỰC NINH, TỈNH NAM ĐỊNH
ỦY BAN NHÂN DÂN XÃ TRỰC ĐẠO

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ
HỆ THỐNG MẠNG LAN CỦA
ỦY BAN NHÂN DÂN XÃ TRỰC ĐẠO

Trực Đạo, năm 2024

ỦY BAN NHÂN DÂN HUYỆN TRỰC NINH, TỈNH NAM ĐỊNH
ỦY BAN NHÂN DÂN XÃ TRỰC ĐẠO

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ
HỆ THỐNG MẠNG LAN CỦA
UBND XÃ TRỰC ĐẠO

Đơn vị vận hành HTTT
UBND xã Trục Đạo

Đơn vị thẩm định hồ sơ
Sở Thông tin và Truyền thông

CHỦ TỊCH UBND XÃ
Nguyễn Thành Nam

Trục Đạo, năm 2024

MỤC LỤC

THUẬT NGỮ, TỪ VIẾT TẮT	1
DANH MỤC CÁC BẢNG	2
DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ	3
PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN ...	4
1. Thông tin Chủ quản hệ thống thông tin.....	4
2. Thông tin Đơn vị vận hành.....	4
3. Mô tả phạm vi, quy mô của hệ thống	4
4. Mô tả cấu trúc của hệ thống.....	5
4.1. Mô hình logic tổng thể	5
a) Sơ đồ hiện trạng	5
b) Sơ đồ quy hoạch mới đáp ứng yêu cầu an toàn	6
4.2. Mô hình kết nối vật lý	7
a) Sơ đồ hiện trạng	7
4.3. Danh mục thiết bị sử dụng trong hệ thống	8
a) Thiết bị hiện có	8
a) Thiết bị cần trang bị để đáp ứng yêu cầu an toàn	9
4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống.....	9
4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống.....	9
PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT	10
1. Danh mục hệ thống thông tin và cấp độ đề xuất.....	10
2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin.....	10
PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM	11
AN TOÀN HỆ THỐNG THÔNG TIN.....	11
PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 1.....	13
5.1.1. Thiết lập chính sách an toàn thông tin.....	13
5.1.2. Tổ chức bảo đảm an toàn thông tin.....	14

5.1.3. Bảo đảm nguồn nhân lực.....	15
5.1.4. Quản lý thiết kế, xây dựng hệ thống thông tin.....	17
5.1.5. Quản lý vận hành hệ thống thông tin.....	18
5.1.6. Phương án Quản lý rủi ro an toàn thông tin.....	19
5.1.7. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin.....	19
PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG CẤP ĐỘ 1.....	21
5.2.1. Bảo đảm an toàn mạng.....	21
5.2.2. Bảo đảm an toàn máy chủ.....	23
5.2.3. Bảo đảm an toàn ứng dụng.....	23
5.2.4. Bảo đảm an toàn dữ liệu.....	24

THUẬT NGỮ, TỪ VIẾT TẮT

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

DANH MỤC CÁC BẢNG

Bảng 1. Danh mục thiết bị sử dụng trong hệ thống	9
--	---

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

Hình 1. Cấu trúc logic của hệ thống	6
Hình 2. Kết nối vật lý của hệ thống	8

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

1. Thông tin Chủ quản hệ thống thông tin

- **Tên Tổ chức:** Ủy ban nhân dân tỉnh Nam Định
- Quy định chức năng, nhiệm vụ và quyền hạn: Luật Tổ chức chính quyền địa phương
- Người đại diện: Ông Phạm Đình Nghị, Chức vụ: Chủ tịch UBND tỉnh.
- Địa chỉ: 57 đường Vị Hoàng, thành phố Nam Định.
- Thông tin liên hệ: Số điện thoại: (0228)3849315 Fax: (0228)3867059

2. Thông tin Đơn vị vận hành

- **Tên Đơn vị vận hành:** Xã Trục Đạo, huyện Trục Ninh.
- Quy định chức năng, nhiệm vụ và quyền hạn: Luật Tổ chức Chính quyền địa phương ngày 19/6/2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;
- Người đại diện: Ông Nguyễn Thành Nam, Chức vụ: Phó Bí thư Đảng ủy, Chủ tịch UBND xã Trục Đạo.
- Địa chỉ:
Xóm Quang Tiến, xã Trục Đạo, huyện Trục Ninh, tỉnh Nam Định.
- Thông tin liên hệ: Số điện thoại: 0915657009

Thư điện tử: xatrucdao.tnh@namdinh.gov.vn

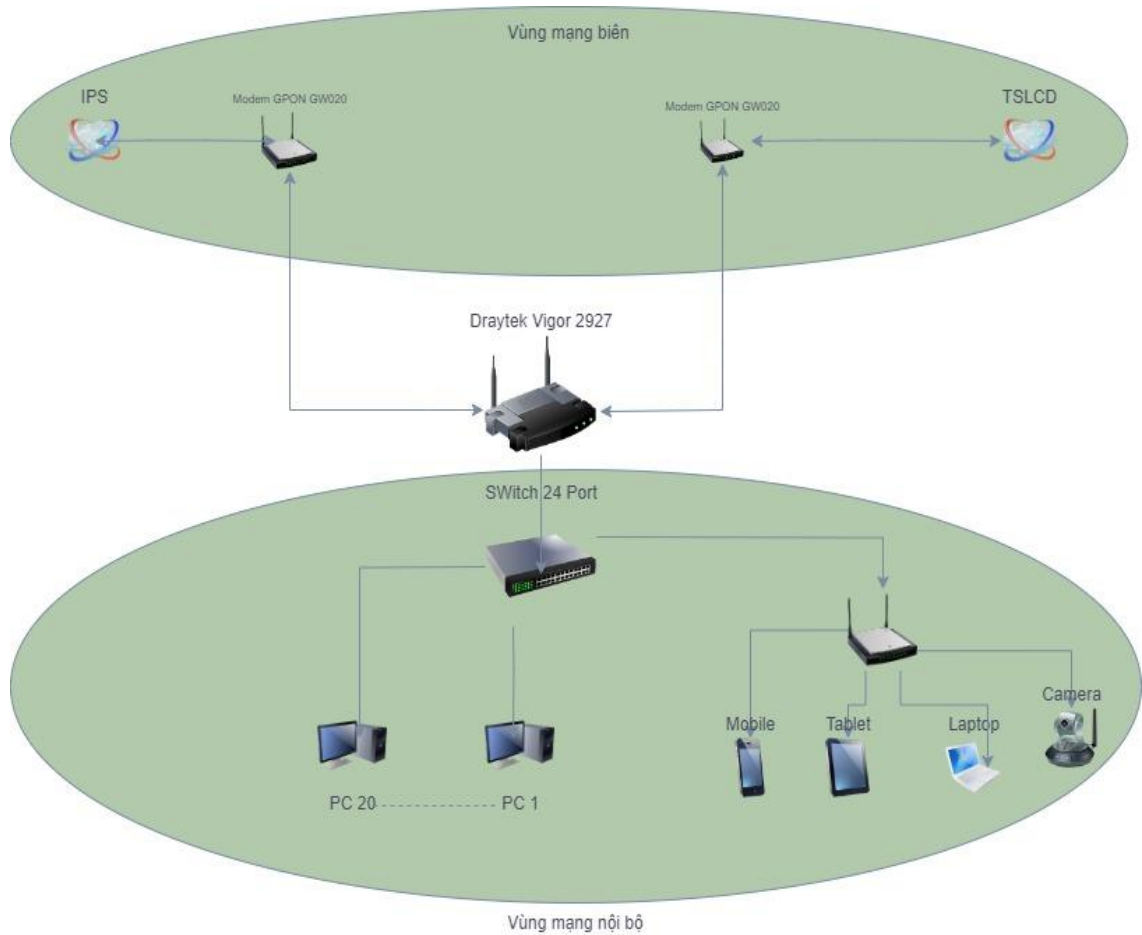
3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống Mạng LAN: Hệ thống thông tin của xã Trục Đạo được thiết lập để phục vụ công tác ứng dụng công nghệ thông tin, chuyển đổi số của xã Trục Đạo.
- Đối tượng phục vụ của hệ thống: công chức, viên chức và người lao động của xã Trục Đạo.

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

1. ISP: Internet service Provide (IP động)

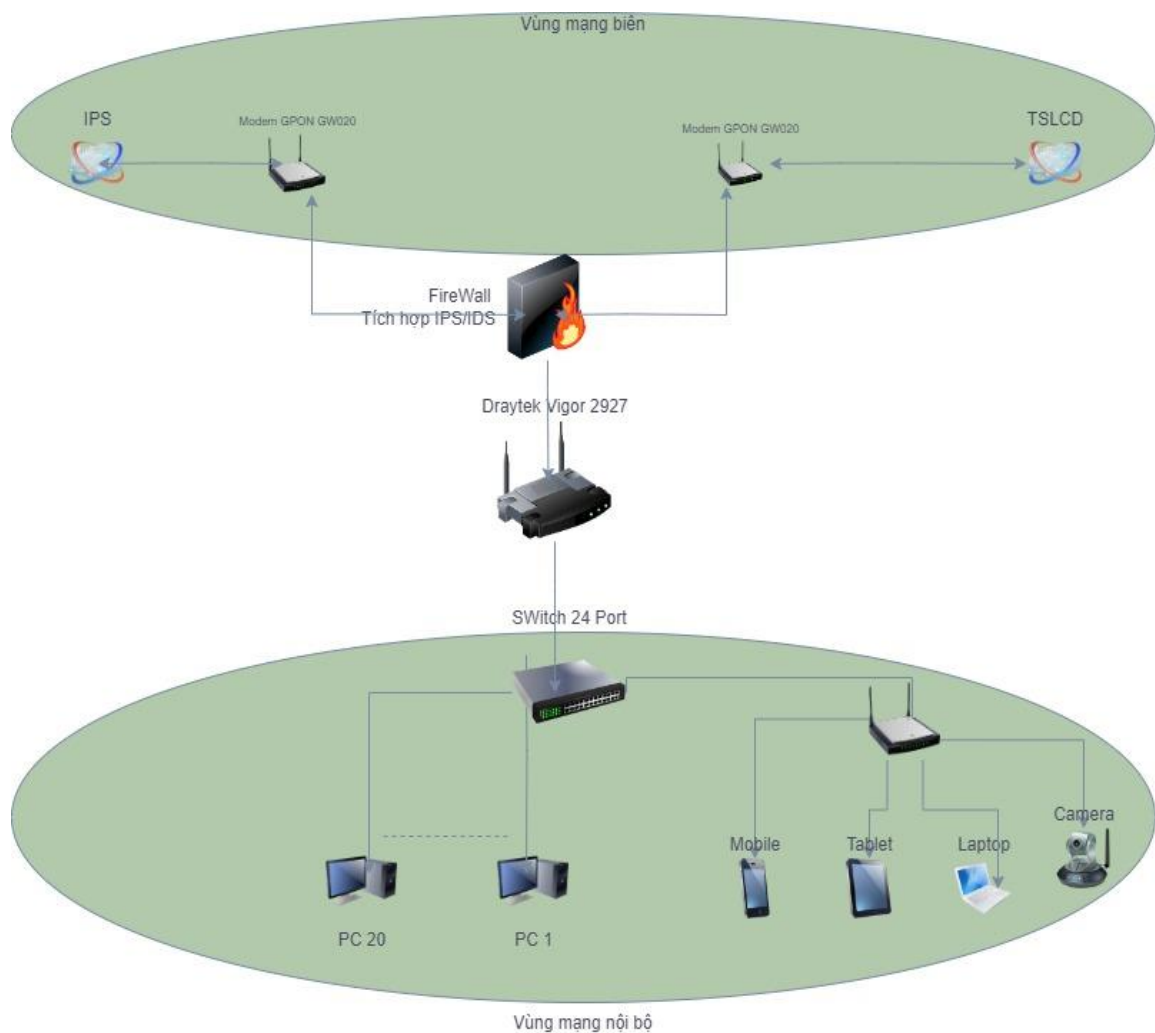
2. Mạng TSLCD

- Modem: I Gate

- G 0/1 WAN TSLCD DRAYTEK Vigor 2927

- LAN tsld DRAYTEK Vigor 2927

- Dải Lan: 10.120.163.192/26 (Vùng mạng nội bộ)



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.

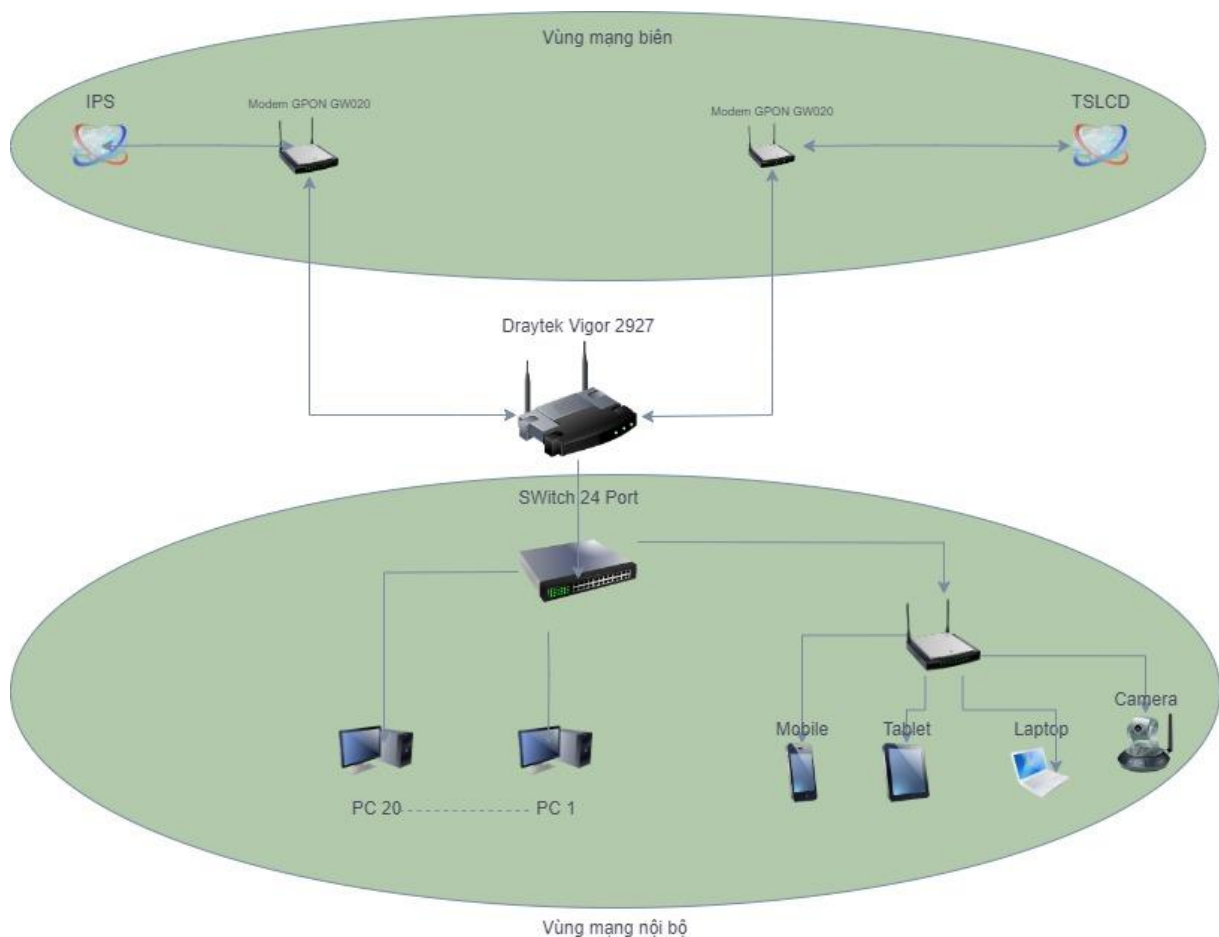
+ Vùng mạng nội bộ đặt các thiết bị nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống.

+ Không thể hiện vùng DMZ do Hệ thống không có các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet.

4.2. Mô hình kết nối vật lý

a) Sơ đồ hiện trạng

1. ISP: Internet service Provide (IP động)
2. Modem: I Gate
3. Modem: DRAYTEK Vigor 2927
4. Switch TP Link
5. Máy tính, Laptop, Wifi



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

1. ISP: Internet service Provide (IP động)

2. Mạng TSLCD

a. 0/1: Modem Igate

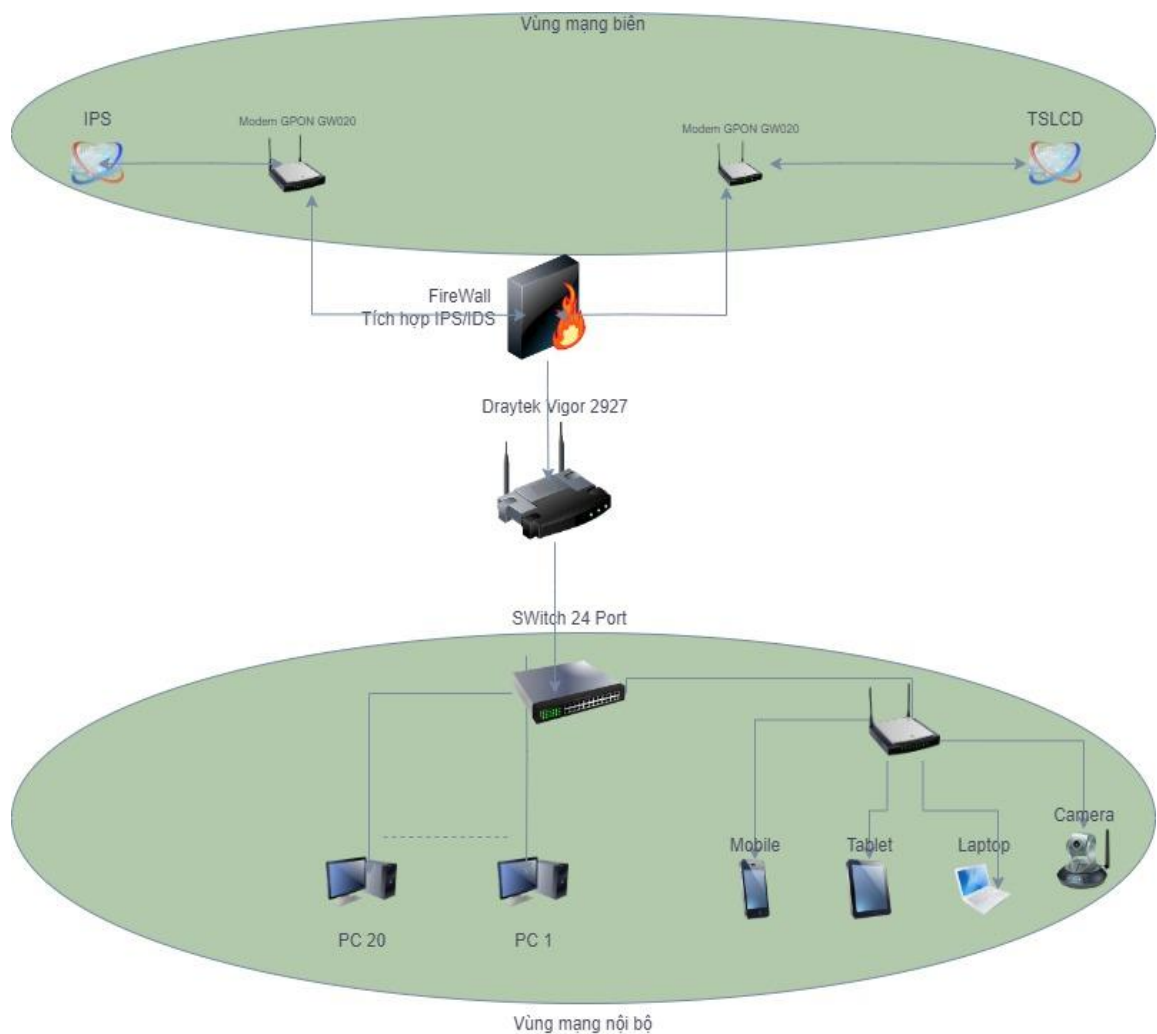
b. Firewall01 tích hợp trên DRAYTEK Vigor 2927

+ wan tslcd Draytek Vigor 2927

Dải Lan 10.120.163.192/26 (Vùng mạng nội bộ)

+ Wifi: Tplink

+ Máy tính, Laptop (IP động)



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/I Gate	Vùng mạng biên	Kết nối và định tuyến động với các Router của ISP.
2	Router Draytek Vigor 2927	Vùng Core	Định tuyến, quản lý truy cập vào/ra và bảo vệ các vùng mạng
3	Switch TP Link	Vùng mạng nội bộ	Thiết bị định tuyến vùng mạng nội bộ
4	Wifi/Tplink TL-W840N (VN)	Vùng mạng nội bộ	Thiết bị cung cấp kết nối internet không dây cho vùng mạng nội bộ
5	PC/Laptop 18/01	Vùng mạng nội bộ	Máy tính phục vụ công việc
6	Camera 03 cái	Vùng mạng nội bộ	<i>Thiết bị khác: các IP camera đơn lẻ, máy in, scan, photocopy kết nối qua cổng LAN (nếu có)</i>

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

a) 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 (Fortigate 200F) (Dự kiến lắp đặt)	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

Không có

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	10.120.163.192/26	IP động

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 xã Trục Đạo, huyện Trục Ninh bao gồm hệ thống thành phần với cấp độ đề xuất tương ứng, bao gồm:

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

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

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

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

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

1. Thiết lập chính sách an toàn thông tin
2. Tổ chức bảo đảm an toàn thông tin
3. Bảo đảm nguồn nhân lực
4. Quản lý thiết kế, xây dựng hệ thống
5. Quản lý vận hành hệ thống
- Quản lý an toàn mạng
- Quản lý an toàn dữ liệu

Đối với những yêu cầu quản lý chưa đáp ứng các yêu cầu an toàn trong Thuyết minh này, Đơn vị vận hành sẽ cập nhật, bổ sung trình Chủ quản hệ thống thông tin ban hành **trong vòng 01 tháng**, kể từ khi HSDXCD được phê duyệt.

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

1. Bảo đảm an toàn mạng
 - 1.1. Thiết kế hệ thống
 - 1.2. Kiểm soát truy cập từ bên ngoài mạng
 - 1.3. Nhật ký hệ thống
 - 1.4. Phòng chống xâm nhập
 - 1.5. Bảo vệ thiết bị hệ thống
2. Bảo đảm an toàn ứng dụng
 - 2.1. Xác thực
 - 2.2. Kiểm soát truy cập
 - 2.3. Nhật ký hệ thống
3. Bảo đảm an toàn dữ liệu

Đối với các yêu cầu kỹ thuật chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, Đơn vị vận hành sẽ triển khai nâng cấp, thiết lập cấu hình hệ thống để đáp ứng yêu cầu **trong vòng 12 tháng**, kể từ khi HSDXCD được phê duyệt.

Thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống của xã Trục Đạo, huyện Trục Ninh, tỉnh Nam Định sẽ bao gồm các thuyết minh thành phần sau:

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

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

5.1.1. Thiết lập chính sách an toàn thông tin

5.1.1.1. Chính sách an toàn thông tin

Yêu cầu	Xây dựng chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống nhằm bảo đảm tính sẵn sàng của hệ thống trong quá trình vận hành, khai thác.
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Tại Quy chế Bảo đảm an toàn hệ thống thông tin hệ thống mạng nội bộ thuộc Ủy ban nhân dân xã Trục Đạo, huyện Trục Ninh ban hành kèm theo Quyết định số: 86/QĐ-UBND ngày 25/09/2024 của UBND xã Trục Đạo, huyện Trục Ninh (<i>sau đây gọi là Quy chế số 86</i>).</p> <p>Quản lý an toàn hệ thống thông tin mạng: (<i>Quy định tại Điều 9, Điều 10, Điều 11, Điều 12, Điều 13, Điều 14, Điều 15, Điều 16, Điều 17 của Quy chế 86</i>).</p>

5.1.1.2. Xây dựng và công bố

Yêu cầu	Chính sách được tổ chức/ bộ phận được ủy quyền thông qua trước khi công bố áp dụng.
Hiện trạng	Đáp ứng
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin trình người đứng đầu đơn vị vận hành ban hành (<i>Quy chế 86</i>)

5.1.1.3. Rà soát, sửa đổi

Yêu cầu	Chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:</p> <p>Định kỳ hàng năm 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 (<i>Điều 21, Quy chế 86</i>)</p>

5.1.2. Tổ chức bảo đảm an toàn thông tin

5.1.2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Phân công công chức có trình độ chuyên môn, am hiểu công nghệ thông tin có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin
Hiện trạng	Đáp ứng
Phương án	<p>1. Sở Thông tin và Truyền thông là đơn vị chuyên trách về an toàn thông tin của UBND tỉnh Nam Định.</p> <p>2. Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống của xã Trực Đạo, bao gồm những nội dung sau:</p> <p>Giao Công chức phụ trách Văn hóa và Thông tin là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin.</p>

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

Yêu cầu 5.1.2.2.a	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin;
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:</p> <p>Giao Công chức phụ trách Văn hóa và Thông tin là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin. Văn phòng HĐND và UBND xã là đơn vị vận hành Hệ thống thông tin (<i>Điều 18, Quy chế số 86</i>)</p>
Yêu cầu 5.1.2.2.b	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống (<i>Điều 18, Quy chế số 86</i>) bao gồm những nội dung sau:</p> <p>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:</p> <p>a) Sở Thông tin và Truyền thông tỉnh Nam Định</p> <p>- Người liên hệ/bộ phận: Trung tâm Chuyển đổi số và Truyền thông</p>

	<p>+ Số điện thoại: 0228. 363 1116</p> <p>+ Email: trungtamcntttt.nd@gmail.com</p> <p>b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)</p> <p>- Người liên hệ/bộ phận: Phòng Ứng cứu sự cố</p> <p>- Số điện thoại: 0869 100 317</p> <p>- Email: ir@vncert.vn</p> <p>- Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn</p> <p>- Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn</p>
--	---

5.1.3. Bảo đảm nguồn nhân lực

5.1.3.1. Tuyển dụng

Yêu cầu	Công chức 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
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại Quy chế 86 quy định:</p> <p>Công chức 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 hoặc phù hợp với vị trí tuyển dụng.</p>

5.1.3.2. Trong quá trình làm việc

Yêu cầu 5.1.3.2.a	Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại Điều 5, Quy chế 86 quy định:</p> <p>1. Quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin trong quá trình làm việc:</p> <p>a. Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống</p> <p>- Với người sử dụng:</p> <p>+ Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra</p>

	<p>khả năng đáp ứng với các yêu cầu về ATTT.</p> <ul style="list-style-type: none"> + Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT. + Cá nhân, tổ chức có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị. - Với cán bộ quản lý và vận hành hệ thống + Cán bộ quản lý và vận hành hệ thống phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin. + Cán bộ quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin. + 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 đảm bảo 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. <p>c. Định kỳ hàng năm, người sử dụng và bộ phận quản lý và vận hành hệ thống được tổ chức đào tạo các kỹ năng về an toàn thông tin theo chương trình, nội dung tại Quyết định số 21/QĐ-TTg ngày 06/01/2021 của Thủ tướng Chính Phủ.</p>
Yêu cầu 5.1.3.2.b	Có hình thức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại Quy chế 86 quy định:</p> <p>Định kỳ hàng năm người sử dụng được tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin theo chương trình, nội dung tại Quyết định số 1907/QĐ-TTg ngày 23/11/2020 của Thủ tướng Chính Phủ.</p>

5.1.3.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu	Cán bộ, công chức chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác
----------------	--

	(nếu có) thuộc sở hữu của tổ chức.
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại Điều 5, Quy chế 86 quy định:</p> <p>Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:</p> <p>a) Cán bộ nghỉ 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 thuộc sở hữu của tổ chức.</p> <p>b) Cán bộ quản trị vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.</p> <p>c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.</p>

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

5.1.4.1. Thiết kế an toàn hệ thống thông tin

Yêu cầu 5.1.4.1.a	Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại khoản 1 Điều 6, Quy chế 86 quy định:</p> <p>Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.</p>
Yêu cầu 5.1.4.1.b	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại khoản 2 Điều 6, Quy chế 86 quy định:</p> <p>Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.</p>

5.1.4.2. Thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai
----------------	--

	thác sử dụng.
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại khoản 1 Điều 8, Quy chế 86 quy định:</p> <p>Quy định đối với việc thử nghiệm và nghiệm thu hệ thống:</p> <ol style="list-style-type: none"> 1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống. 2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.

5.1.5. Quản lý vận hành hệ thống thông tin

5.1.5.1. Quản lý an toàn mạng

Yêu cầu	Xây dựng và thực thi chính sách, quy trình quản lý vận hành hoạt động bình thường của hạ tầng mạng.
Hiện trạng	Đáp ứng
Phương án	<p>Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại khoản 1 Điều 9, Quy chế 86 quy định:</p> <p>Quy định về quản lý an toàn mạng:</p> <ol style="list-style-type: none"> a. 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. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, đảm bảo tính khả dụng của hệ thống. b. 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. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc. c. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống. Việc cài đặt, kết nối và gỡ bỏ thiết bị mạng trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

5.1.5.2. Quản lý an toàn máy chủ và ứng dụng

Yêu cầu	Xây dựng và thực thi chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.
Hiện trạng	Đáp ứng
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại Quy chế số 86.

5.1.5.3. Quản lý an toàn dữ liệu

Yêu cầu	Có phương án sao lưu dự phòng thông tin, dữ liệu, cấu hình hệ thống.
Hiện trạng	Đáp ứng
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, Điều 10, Quy chế số 86 quy định về quản lý an toàn dữ liệu.

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

Yêu cầu	Có chính sách, quy trình quản lý quản lý rủi ro an toàn thông tin
Hiện trạng	Đáp ứng
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống tại Điều 16, Quy chế 86 quy định về quản lý rủi ro an toàn thông tin.

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

Yêu cầu	Có quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ
Hiện trạng	Đáp ứng
Phương án	<p>Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, tại Điều 17, Quy chế 86.</p> <ol style="list-style-type: none"> 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 xóa 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 cán bộ của xã Trục Đạo, huyện Trục Ninh. Căn cứ theo quy định tại Điều 7/NĐ85, hệ thống này được đề xuất cấp độ 1.

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

5.2.1. Bảo đảm an toàn mạng

5.2.1.1. Thiết kế hệ thống

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

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng nội bộ	Có	Cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối, các thiết bị khác của người sử dụng vào hệ thống
2	Vùng mạng biên	Có	Cung cấp các kết nối với mạng Internet và mạng diện rộng
3	Vùng DMZ	N/A	Hệ thống không có các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet.

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	N/A	Không cho phép truy cập, quản trị hệ thống từ xa.
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Có	Thiết lập cấu hình chức năng quản lý truy cập giữa vùng mạng LAN và mạng biên trên bộ định tuyến. Thiết bị định tuyến/ tường lửa chưa được cấu hình chức năng IDS/IPS. Dự kiến thiết lập cấu hình hệ thống đáp ứng yêu cầu trong vòng 12 tháng, kể từ khi HSĐXCĐ

			được phê duyệt.
3	Phương án phòng chống mã độc cho máy chủ và máy trạm	Có	Cài đặt phần mềm phóng, chống mã độc cho toàn bộ máy chủ/máy trạm có trong hệ thống sử dụng giải pháp AV (hoặc EDR) của hãng ... (Hệ thống diệt vi rút chưa cài đồng bộ, dự kiến thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong vòng 12 tháng, kể từ khi HSDXCĐ được phê duyệt.

5.2.1.2. Kiểm soát truy cập từ bên ngoài mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet	Có	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.

5.2.1.3. Nhật ký hệ thống

Yêu cầu	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị mạng chính
Thiết bị	
Modem/I Gate	+
Router Draytek Vigor 2927	+
Switch TP Link	+
Wifi/Tplink TL-W840N (VN)	+

5.2.1.4. Phòng chống xâm nhập

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống xâm nhập để bảo vệ vùng DMZ	Có	Hệ thống không có các máy chủ công cộng, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet
2	Định kỳ cập nhật cơ sở dữ	Có	Firewall01 có bản quyền cho chức

	liệu dấu hiệu phát hiện tấn công mạng		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. Dự kiến thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong vòng 12 tháng, kể từ khi HSĐXCĐ được phê duyệt.
--	---------------------------------------	--	--

5.2.1.5. 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/Router Draytek		+	+
Switch TP Link		+	+
Wifi/TPLink		+	+

5.2.2. Bảo đảm an toàn máy chủ

(Hiện tại trong Hệ thống nội bộ không có máy chủ)

5.2.3. Bảo đảm an toàn ứng dụng

5.2.3.1. Xác thực

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

5.2.3.2. Kiểm soát truy cập

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

5.2.3.3. Nhật ký hệ thống

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

5.2.4. Bảo đảm an toàn dữ liệu

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...