UBND THỊ XÃ ĐỨC PHỔ

UBND PHƯỜNG PHỔ HÒA

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 1
HỆ THỐNG THÔNG TIN MẠNG NỘI BỘ (LAN)
CỦA UBND PHƯỜNG PHỔ HÒA

Phổ Hòa, ngày 10 tháng 6 năm 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
4.	VPN	Vitural Private Network
5.	DNS	Domain Name Server

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

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

1. Thông tin liên hệ

a) Tên hệ thống thông tin: Hệ thống mạng nội bộ của UBND phường Phổ Hòa.

b) Chủ quản hệ thống thông tin: Ủy ban nhân dân phường Phổ Hòa.

Người đại diện: Ông Phạm Ngọc Thạch, Chức vụ: Chủ tịch.

Địa chỉ: 133 đường Phạm Xuân Hòa, phường Phổ Hòa, thị xã Đức Phổ, tỉnh Quảng Ngãi.

Thông tin liên hệ: 0255.3859404; Email: vanphongubndxaphohoa@gmail.com.

2. Đơn vị vận hành hệ thống thông tin: UBND phường Phổ Hòa

- Người đại diện: Ông Phạm Ngọc Thạch, Chức vụ: Chủ tịch UBND phường Phổ Hòa.

- Địa chỉ: 133 đường Phạm Xuân Hòa, phường Phổ Hòa, thị xã Đức Phổ, tỉnh Quảng Ngãi.

Thông tin liên hệ: 0255.3859404; Email: vanphongubndxaphohoa@gmail.com.

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống thông tin: Phục vụ nội bộ UBND phường được thiết lập để phục vụ hoạt động quản trị, vận hành nội bộ của cơ quan.

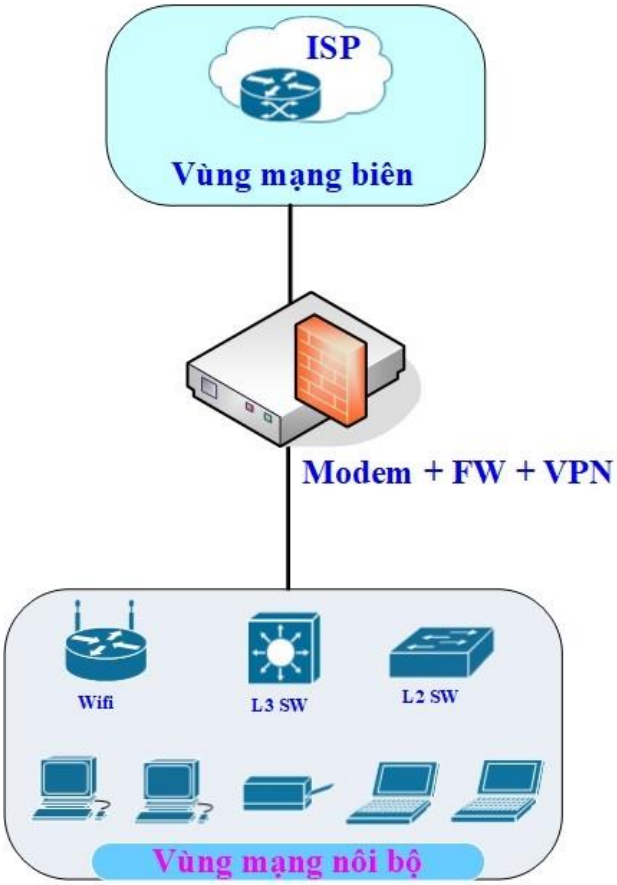
- Đối tượng phục vụ của hệ thống: Cơ quan, tổ chức, doanh nghiệp trên địa bàn UBND phường Phổ Hòa.

- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi trung tâm tích hợp dữ liệu:

+ Hệ thống mạng nội bộ.

4. Mô tả cấu trúc của hệ thống

4.1. Mô hình logic tổng thể



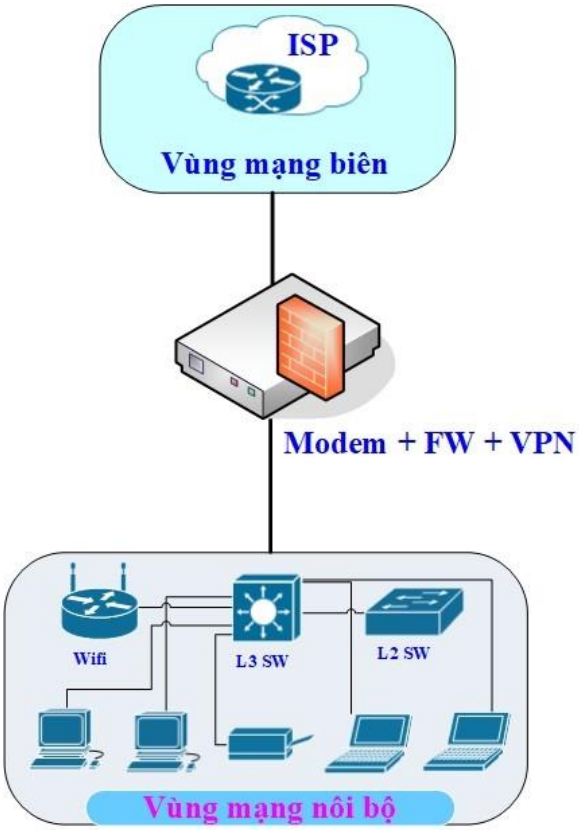
Hình 1. Cấu trúc logic của hệ thống

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



Hình 2. Kết nối vật lý của hệ thống

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	Vùng mạng biên	Kết nối và định tuyến động với các Router của ISP.
2	Igate GW040	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.
3	TP link TL/SG1024G	Vùng mạng nội bộ	Chuyển mạch trung tâm đảm bảo tốc độ vận chuyển và liên kết với các lớp mạng

4	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

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	192.168.1.1/18	8.8.8.8
2	Vùng mạng biên	192.168.1.1 255.255.255.0	8.8.4.4

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 UBND phường Phổ Hòa 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 nội bộ	1	Điều 7 NĐ85/2016

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

Hệ thống Mạng nội bộ chỉ xử lý thông tin công khai và phục vụ hoạt động nội bộ cho cán bộ của UBND phường Phổ Hòa. 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 vận hành hệ thống:

- Quản lý an toàn mạng.

- Quản lý an toàn máy chủ và ứng dụng.

- Quản lý an toàn dữ liệu.

5. Phương án quản lý rủi ro an toàn thông tin:

6. Phương án kết thúc vận hành, khai thác, thanh lý, hủy bỏ:

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 06 tháng, kể từ khi hồ sơ ĐXCĐ được phê duyệt.

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

1. Bảo đảm an toàn dữ liệu.

1.1. Sao lưu dự phòng:

Đối với các yêu cầu kỹ thuật chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, đơn vị vận hành sẽ triển khai nâng cấp, thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong vòng 18 tháng, kể từ khi hồ sơ ĐXCĐ được phê duyệt.

Thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống của UBND phường Phổ Hòa 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 nội bộ	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, đơn vị vận hành xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống.
Phương án	Quy chế bảo đảm an toàn thông tin, an ninh mạng đã bao gồm các yêu cầu, bao gồm: 1. Quản lý an toàn mạng: a) Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật. b) Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (*có thể tích hợp tường lửa trên modem hoặc router*) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng. 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 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, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành.

	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. 3. 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, thiết bị di động thông minh) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích riêng. 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) Đơn vị/bộ phận giao nhiệm vụ chuyên trách về an toàn thông tin phải thường xuyên theo dõi, kiểm tra các lỗ hổng bảo mật và quản lý kết nối, truy cập khi sử dụng thiết bị đầu cuối từ xa. e) Đơn vị/bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc. f) Đơn vị/bộ phận chuyên trách về an toàn thông tin thường xuyên theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng.

5.1.1.2. Xây dựng và công bố

Yêu cầu	Chính sách được tổ chức/ bộ phận được ủy quyền thông qua trước khi công bố áp dụng.
Hiện trạng	Đáp ứng/đơn vị vận hành đã xây dựng, Quy chế bảo đảm an toàn thông tin, an ninh mạng.
Phương án	Xây dựng và công bố Quy chế bảo đảm an toàn thông tin: 1. Quy chế được lấy ý kiến cấp có thẩm quyền, đơn vị liên quan trước khi công bố áp dụng. 2. Quy chế được xây dựng trình Chủ tịch UBND phường Phổ Hòa ban hành.

5.1.1.3. Rà soát, sửa đổi

Yêu cầu	Chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.
Hiện trạng	Đáp ứng. Tham chiếu điều 22 Quy chế bảo đảm an toàn, an ninh mạng.
Phương án	Rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin: 1. Định kỳ 03 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. 2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời Bộ phận chuyên trách về ATTT để tổng hợp báo cáo, điều chỉnh, bổ sung.

5.1.2. Tổ chức bảo đảm an toàn thông tin

5.1.2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Có cán bộ có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin.
Hiện trạng	Đáp ứng. Tham chiếu điều 23 Quy chế bảo đảm an toàn, an ninh mạng.
Phương án	a) Giao công chức Văn phòng - Thống kê là đơn vị chuyên trách về an toàn thông tin cho hệ thống. b) Công chức Văn phòng - Thống kê chủ trì, phối hợp với các bộ phận và đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của lãnh đạo UBND phường.

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

Yêu cầu 5.1.2.2.a	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin;
Hiện trạng	Đáp ứng, tham chiếu điều 4 Quy chế bảo đảm an toàn, an ninh mạng.

Phương án	Phối hợp với những cơ quan/tổ chức có thẩm quyền: 1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin: a) Giao bộ phận Văn phòng - Thống kê là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin. b) Bộ phận Văn phòng - Thống kê làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn phường. c) Bộ phận Văn phòng - Thống kê phối hợp với các đơn vị chuyên trách về ATTT của tỉnh, Đội ứng cứu sự cố ATTT mạng tỉnh, UBND thị xã Đức Phổ và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh. 2. 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: Tùy theo mức độ sự cố, phối hợp Tổ ứng cứu an toàn thông tin huyện hoặc đội ứng cứu an toàn thông tin tỉnh và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.
Yêu cầu 5.1.2.2.b	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin.
Hiện trạng	Đáp ứng. Tham chiếu điều 4, điều 14 Quy chế bảo đảm an toàn, an ninh mạng hệ thống ...
Phương án	- Giao công chức Văn phòng - Thống kê làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý sự cố về an toàn thông tin mạng đối với Hệ thống thông tin của UBND phường Phổ Hòa. - 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: Tùy theo mức độ sự cố, phối hợp Tổ ứng cứu an toàn thông tin huyện hoặc Đội ứng cứu an toàn thông tin tỉnh và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

5.1.3. Bảo đảm nguồn nhân lực

5.1.3.1. Tuyển dụng

Yêu cầu	Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng.
Hiện trạng	Đáp ứng. Tham chiếu điều 5 Quy chế bảo đảm an toàn, an ninh mạng.
Phương án	Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ: Cán bộ được tuyển dụng, bố trí vào vị trí việc làm về an toàn thông tin có trình độ, năng lực lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng được lồng ghép trong quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

5.1.3.2. Trong quá trình làm việc

Yêu cầu 5.1.3.2.a	Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống.
Hiện trạng	Đáp ứng. Tham chiếu điều 5 Quy chế bảo đảm an toàn, an ninh mạng.
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 người sử dụng, cán bộ quản lý và vận hành hệ thống. a) Với người sử dụng: - 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 khả năng đáp ứng các yêu cầu về ATTT. - Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT. - Chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng

	trực tuyến tin cậy và các thông tin phù hợp với chức năng, chức trách, quyền hạn của mình; không truy cập, mở các thông tin, thư điện tử không rõ nguồn gốc. - Có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẽ mật khẩu với người khác. Đặt mật khẩu với độ an toàn cao và thay đổi mật khẩu tối thiểu 03 lần/tháng; các tài khoản đăng nhập các hệ thống phải được đăng xuất khi không sử dụng. Thực hiện các biện pháp mã hóa đối với các tài khoản, mật khẩu được lưu trữ trên thiết bị. - Khóa máy tính tạm thời khi rời khỏi nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan. b) Trách nhiệm bảo đảm an toàn thông tin cho cán bộ quản lý và vận hành hệ thống. - 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. - 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. - Các bộ phận, cá nhân tham gia sử dụng 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.
Yêu cầu 5.1.3.2.b	Có hình thức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.
Hiện trạng	Đáp ứng. Tham chiếu điều 5 Quy chế bảo đảm an toàn, an ninh mạng.
Phương án	Phải được thường xuyên phổ biến, quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.

5.1.3.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu	Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức.
Hiện trạng	Đáp ứng. Tham chiếu điều 5 Quy chế bảo đảm an toàn, an ninh mạng.
Phương án	Quy định đối với cán bộ nghỉ hoặc thay đổi công việc: 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. b) Vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

5.1.4. Quản lý vận hành hệ thống thông tin

5.1.4.1. Quản lý an toàn mạng

Yêu cầu	Xây dựng và thực thi chính sách, quy trình quản lý vận hành hoạt động bình thường của hạ tầng mạng.
Hiện trạng	Đáp ứng. Tham chiếu điều 8 Quy chế bảo đảm an toàn, an ninh mạng.
Phương án	Quy định về quản lý an toàn mạng: 1. Quản lý, vận hành hoạt động bình thường của hệ thống: a) Thực hiện việc quản lý và kiểm soát mạng nhằm ngăn ngừa các nguy cơ, rủi ro và duy trì an toàn cho các máy tính, ứng dụng sử dụng mạng: - Có sơ đồ logic và vật lý hệ thống mạng, tổ chức sử dụng 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. - Sử dụng thiết bị tường lửa, thiết bị phát hiện và kiểm soát truy cập từ bên ngoài mạng và phân chia hệ thống mạng thành các

	vùng mạng quản lý theo chính an toàn thông tin riêng; 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. b) Thiết lập, cấu hình đầy đủ các tính năng của thiết bị mạng. Thường xuyên, kiểm tra phiên bản hệ điều hành của thiết bị mạng để cập nhật, vá lỗi khi cần thiết. Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng bảo mật và các truy cập bất hợp pháp vào hệ thống mạng. Thường xuyên kiểm tra, phát hiện những kết nối, trang thiết bị, phần mềm cài đặt bất hợp pháp vào mạng. c) Xác định và ghi rõ các tính năng an toàn, các mức độ bảo mật của dịch vụ và yêu cầu quản lý trong các thỏa thuận về dịch vụ mạng do bên thứ ba cung cấp. d) Mạng không dây (WIFI), thiết lập các thông số an toàn và định kỳ ít nhất 03 tháng thay đổi mật khẩu truy cập nhằm tăng cường cong tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn. 2. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố - Phải có phương án dự phòng đường truyền mạng, thiết bị mạng để đảm bảo tính sẵn sàng đáp ứng yêu cầu hoạt động của hệ thống mạng. - Triển khia hệ thống/phương tiện lưu trữ độc lập để lưu trữ các thông tin cấu hình thiết bị mạng, kết nối, định danh trong mạng để khôi phục sau khi xảy ra sự cố. 3. Truy cập và quản lý cấu hình hệ thống a) Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin 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. b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của tài khoản vi

	phạm. c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng khóa) trước khi đưa vào vận hành, khai thác d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác.

5.1.4.2. 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	Hệ thống thông tin của UBND phường Phổ Hòa không có máy chủ và ứng dụng.
Phương án	

5.1.4.3. Quản lý an toàn dữ liệu

Yêu cầu	Có phương án sao lưu dự phòng thông tin, dữ liệu, cấu hình hệ thống.
Hiện trạng	Đáp ứng. Tham chiếu điều 9 Quy chế bảo đảm an toàn, an ninh mạng.
Phương án	1. 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) a) Lập danh sách các dữ liệu lưu trữ, phần mền cần được sao lưu, có phân loại theo thời gian lưu trữ, phương pháp sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu. b) Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: Đơn vị quản trị hệ thống thực hiện xây dựng tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung

	cấp dịch vụ, hệ thống điều hành mà đơn vị quản lý. 2. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ. a) 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, dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có). b) Thực hiện sao lưu dữ liệu định kỳ: Cán bộ phụ trách sao lưu thực hiện sao lưu định kỳ theo phương án sao lưu đã được phê duyệt. c) Kiểm tra định kỳ: Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.

5.1.5. Phương án Quản lý sự cố an toàn thông tin

Yêu cầu	Có chính sách, quy trình quản lý quản lý sự cố an toàn thông tin.
Hiện trạng	Đáp ứng. Tham chiếu điều 19 Quy chế bảo đảm an toàn, an ninh mạng.
Phương án	1. Xác định mức sự cố: a) Nhận biết tài sản thông qua xác định và thu thập thông tin đầy đủ về tài sản của mình đang quản lý, đặc biệt là các thông tin liên quan đến đặc điểm, nơi lưu trữ, mức độ quan trọng và giá trị, đặc thù của tài sản. Đánh giá các nguy cơ, điểm yếu đối với tài sản đó, từ đó có thể đánh giá xem mỗi tài sản khi gặp rủi ro thì sẽ gây ra hậu quả, mức độ ảnh hưởng thế nào đối với cơ quan tổ chức. b) Phân loại nhóm các điểm yếu: Nhóm các điểm yếu liên quan đến tồn tại lỗ hỏng, điểm yếu an toàn thông tin trong hệ thống; nhóm các điểm yếu liên quan đến thiếu hoặc không đáp ứng các biện pháp quản lý: Không có quy định về sử dụng mật khẩu an toàn; không có quy định về sử dụng mật khẩu an toàn; không có quy định về lưu trữ có mã hóa, không có quy định về quy trình xử lý sự cố, không có quy định về đảm bảo an toàn thông tin phái người sử dụng,…; Nhóm các điểm yêu liên quan đến thiếu hoặc không đáp ứng các biện pháp kỹ thuật: Không có biện pháp phòng chống xâm nhập, không có biện pháp phòng chống mã độc, không có biện pháp phòng chống tấn công,…; Nhóm các

	điểm yếu khác liên quan đến nguy cơ mất an toàn thông tin từ bên thứ ba. c) Phân loại các mối đe dọa: Nhóm các mối đe dọa từ việc tồn tại, điểm yếu, lỗ hổng trong hệ thống; Nhóm các mối đe dọa từ việc từ việc thiếu hoặc không đáp ứng các biện pháp quản lý; Nhóm các mối đe dọa từ việc thiếu hoặc không đáp ứng các biện pháp kỹ thuật. d) Đánh giá hậu quả và khả năng xảy ra sự cố, xác định mức độ rủi ro bao gồm các mức thấp, trung bình, cao, rất cao, cực cao. 2. Quy trình đánh giá và quản lý sự cố bao gồm 04 bước: (1) Thiết lập bối cảnh; (2) Đánh giá rủi ro; (3) Xử lý sự cố; (4) Chấp nhận rủi ro và 02 quá trình thực hiện song song: Truyền thông và tư vấn rủi ro, Giám sát và soát xét sự cố. 3. Biện pháp kiểm soát rủi ro được thực hiện theo yêu cầu an toàn cơ bản trong Hồ sơ đề xuất cấp độ của hệ thống thông tin được cấp có thẩm quyền phê duyệt.

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

Yêu cầu	Có quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.
Hiện trạng	Đáp ứng. Tham chiếu điều 16 Quy chế bảo đảm an toàn, an ninh mạng.
Phương án	1. Khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống phải được Bộ phận chuyên trách an toàn thông tin thực hiện kiểm tra, đánh giá bảo đảm an toàn thông tin. 2. Quá trình xử lý thông tin trên hệ thống phải được thực hiện khi thay đổi mục đích sử dụng hoặc gỡ bỏ theo phương án kỹ thuật được lãnh đạo UBND xã phê duyệt.

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 UBND phường Phổ Hòa. 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 Bảo đảm an toàn dữ liệu

5.2.1. 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