ỦY BAN NHÂN DÂN TỈNH QUẢNG NGÃI
ỦY BAN NHÂN DÂN XÃ ĐĂK PLÔ

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 2
HỆ THỐNG THÔNG TIN
ỦY BAN NHÂN DÂN XÃ ĐĂK PLÔ

Quảng Ngãi – 2026

ỦY BAN NHÂN DÂN TỈNH QUẢNG NGÃI
ỦY BAN NHÂN DÂN XÃ ĐĂK PLÔ

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 2 HỆ THỐNG THÔNG TIN

	Người xây dựng	Người xem xét	Người phê duyệt
Họ tên	A Mạnh	Ma Thị Kìa	Nguyễn Văn Vĩnh
Ký tên			
Chức vụ	Cán bộ phụ trách chuyển đổi số và ATTT - NAM	Phó Chánh Văn phòng phụ trách Văn phòng HĐND-UBND xã	Chủ tịch UBND xã
Ngày	02/6/2026	02/6/2026	02/6/2026

Quảng Ngãi – 2026

Mục Lục

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Nghĩa đầy đủ
01	CNTT	Công nghệ thông tin
02	CSDL	Cơ sở dữ liệu
03	HSĐXCĐ	Hồ sơ đề xuất cấp độ
04	NỘI BỘ	Mạng nội bộ
05	VPN	Virtual Private Network
06	DNS	Domain Name Server
07	UBND	Ủy ban nhân dân dân
08	HĐND	Hội đồng nhân dân

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

1. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: UBND tỉnh Quảng Ngãi.

- Quy định chức năng, nhiệm vụ và quyền hạn của UBND tỉnh: Quy định tại 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 Hoàng Giang, Chức vụ: Chủ tịch UBND tỉnh Quảng Ngãi.

- Địa chỉ: 52 Hùng Vương, Phường Cẩm Thành, tỉnh Quảng Ngãi.

- Thông tin liên hệ:

+ Số điện thoại: 0255 3712 135

+ Thư điện tử: ubnd@quangngai.gov.vn

2. Thông tin Đơn vị vận hành

- Tên Đơn vị vận hành: Ủy ban nhân dân Xã Đăk Plô.

Người đại diện ông: Nguyễn Văn Vĩnh, Chức vụ: Chủ tịch UBND xã.

- Địa chỉ: Thôn Bung Koong, xã Đăk Plô, tỉnh Quảng Ngãi

- Thông tin liên hệ:

+ Số điện thoại: 0985123595

+ Thư điện tử: nvvinh-dakplo@quangngai.gov.vn

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống: Hệ thống thông tin UBND Xã Đăk Plô được triển khai nhằm đáp ứng tổng thể nhu cầu quản lý, điều hành và hỗ trợ quản lý tại UBND. Hệ thống thông tin UBND, HĐND xã Đăk Plô được xây dựng để phục vụ công tác của cán bộ công chức viên chức người lao động, phục vụ công tác chỉ đạo điều hành trong phạm vi UBND, HĐND xã Đăk Plô và phục vụ người dân đến làm việc tại xã. Quy mô sử dụng cho các tổ chức thuộc UBND Xã Đăk Plô.

- Đối tượng phục vụ của Hệ thống:

+ Các đơn vị trực thuộc HĐND, UBND xã Đăk Plô: Bao gồm toàn thể các phòng/ban chuyên môn và đơn vị chức năng trực thuộc, cùng với đội ngũ cán bộ, viên chức và người lao động đang công tác tại HĐND UBND;

+ Cơ quan, tổ chức, cá nhân có nhu cầu kết nối và sử dụng hệ thống mạng internet khi làm việc tại xã: Là các đơn vị phối hợp, cơ quan quản lý cấp trên, các cơ sở liên quan hoặc cá nhân có liên quan đến hoạt động chuyên môn, hành chính, và được phân quyền truy cập, khai thác thông tin theo quy định;

+ Cơ quan, tổ chức, cá nhân tham gia cung cấp dịch vụ kỹ thuật: Bao gồm các đơn vị, doanh nghiệp hoặc cá nhân chịu trách nhiệm quản lý, vận hành, bảo trì, nâng cấp hệ thống mạng nội bộ, đồng thời bảo đảm an toàn thông tin và an ninh mạng, nhằm duy trì hoạt động ổn định, liên tục và hiệu quả của hệ thống tại UBND Xã Đăk Plô.

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

+ Hệ thống mạng nội bộ (LAN): Phục vụ kết nối mạng đến các hệ thống khác phục vụ hoạt động của HĐND UBND;

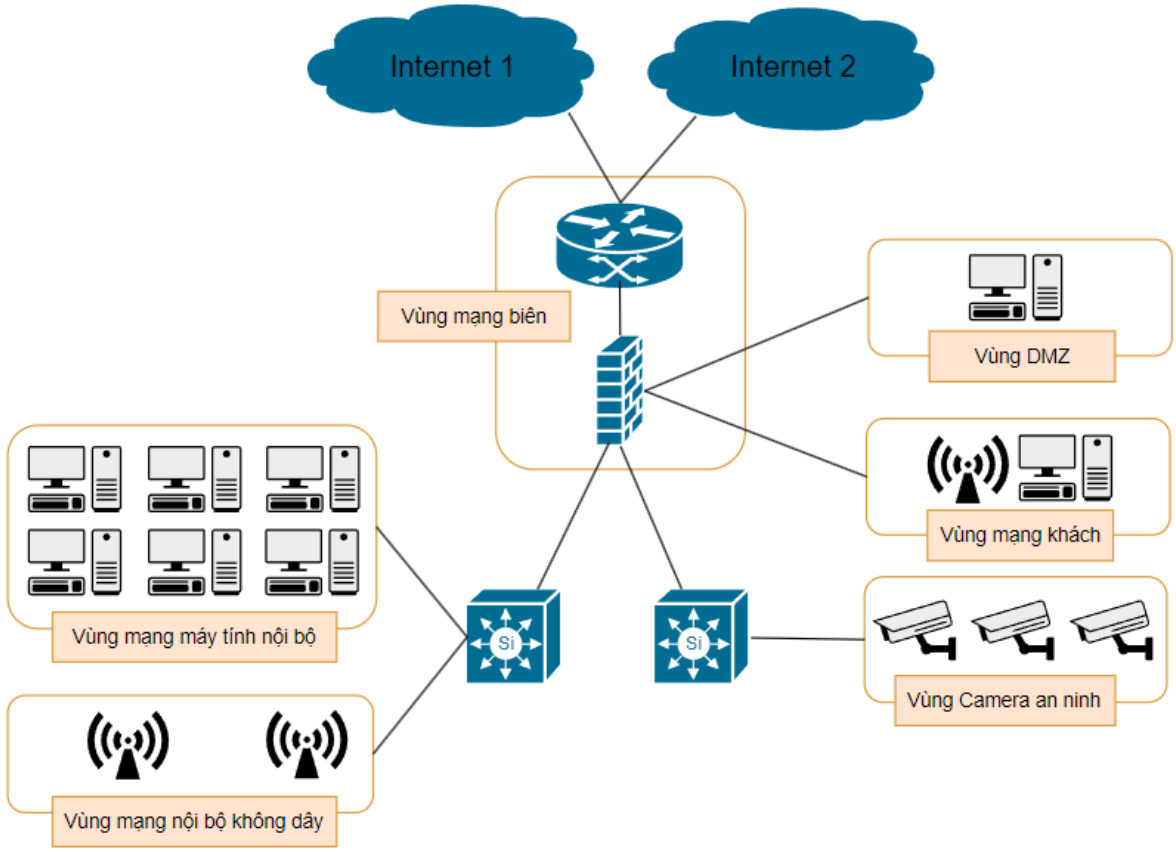
+ Hệ thống camera giám sát: phục vụ công tác giám sát an ninh, an toàn trong khuôn viên cơ quan

+ Hệ thống mạng phục vụ Cơ quan, tổ chức, cá nhân: phục vụ kết nối internet;

4. Mô tả cấu trúc của hệ thống định hướng điều chỉnh đáp ứng ATTT cấp độ 2

4.1. Mô hình tổng thể

a) Mô hình sơ đồ logic hệ thống



Hình 1. Sơ đồ logic của hệ thống

Các vùng mạng được thiết kế như sau:

+ Vùng mạng biên: Đây là khu vực bố trí các thiết bị quan trọng như Router và Firewall, đóng vai trò trung gian giữa hệ thống mạng nội bộ và Internet. Vùng mạng biên chịu trách nhiệm bảo vệ và quản lý toàn bộ lưu lượng ra vào hệ thống, bao gồm kiểm soát truy cập, lọc gói tin, giám sát an ninh và phát hiện, ngăn chặn các mối đe dọa từ bên ngoài;

+ Vùng mạng nội bộ: Đây là khu vực được thiết kế, bố trí các thiết bị như máy tính, máy in và các thiết bị nội bộ khác, cung cấp dịch vụ cho người dùng. Vùng mạng này cho phép kết nối, chia sẻ dữ liệu và truy cập internet một cách an toàn, đảm bảo hiệu suất và bảo mật;

+ Vùng mạng không dây (nội bộ UBND): Được thiết kế, bố trí lắp đặt các thiết bị wifi cung cấp kết nối internet không dây cho nhân viên, cán bộ thuộc UBND xã Đăk Plô. Đảm bảo tách biệt với các vùng mạng khác để tăng cường bảo mật;

+ Vùng mạng khách: Được thiết kế, bố trí lắp đặt các thiết bị wifi cung cấp kết nối internet không dây và máy tính kết nối internet cho người dùng. Vùng

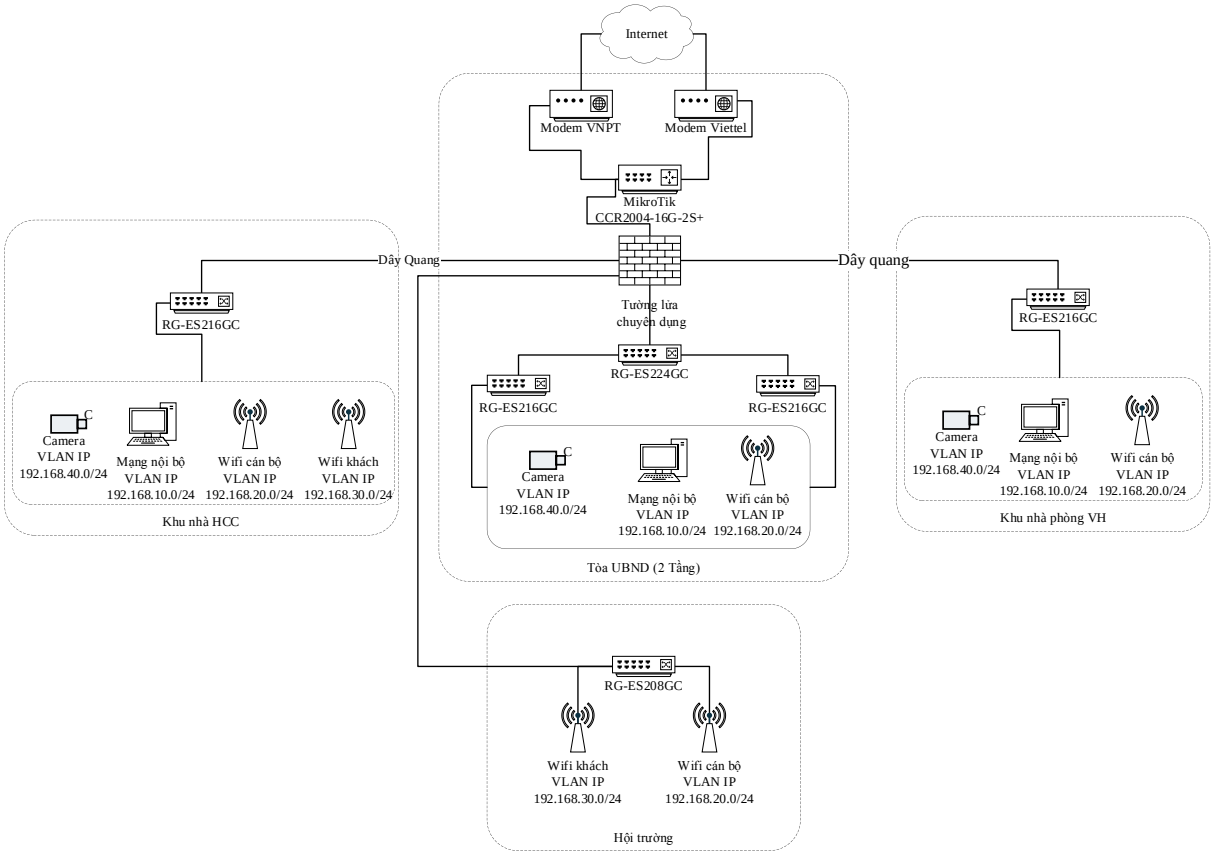
mạng này chỉ cho phép truy cập internet, đảm bảo tách biệt với các vùng mạng khác để tăng cường bảo mật;

+ Vùng mạng Camera an ninh: Vùng mạng dành riêng cho quản trị và truy xuất camera an ninh trong đơn vị.

+ Vùng DMZ: Được thiết kế để cung cấp các dịch vụ truy cập công cộng từ bên ngoài như: web, email,... hoặc là vùng remote mà không làm ảnh hưởng đến hệ thống mạng nội bộ.

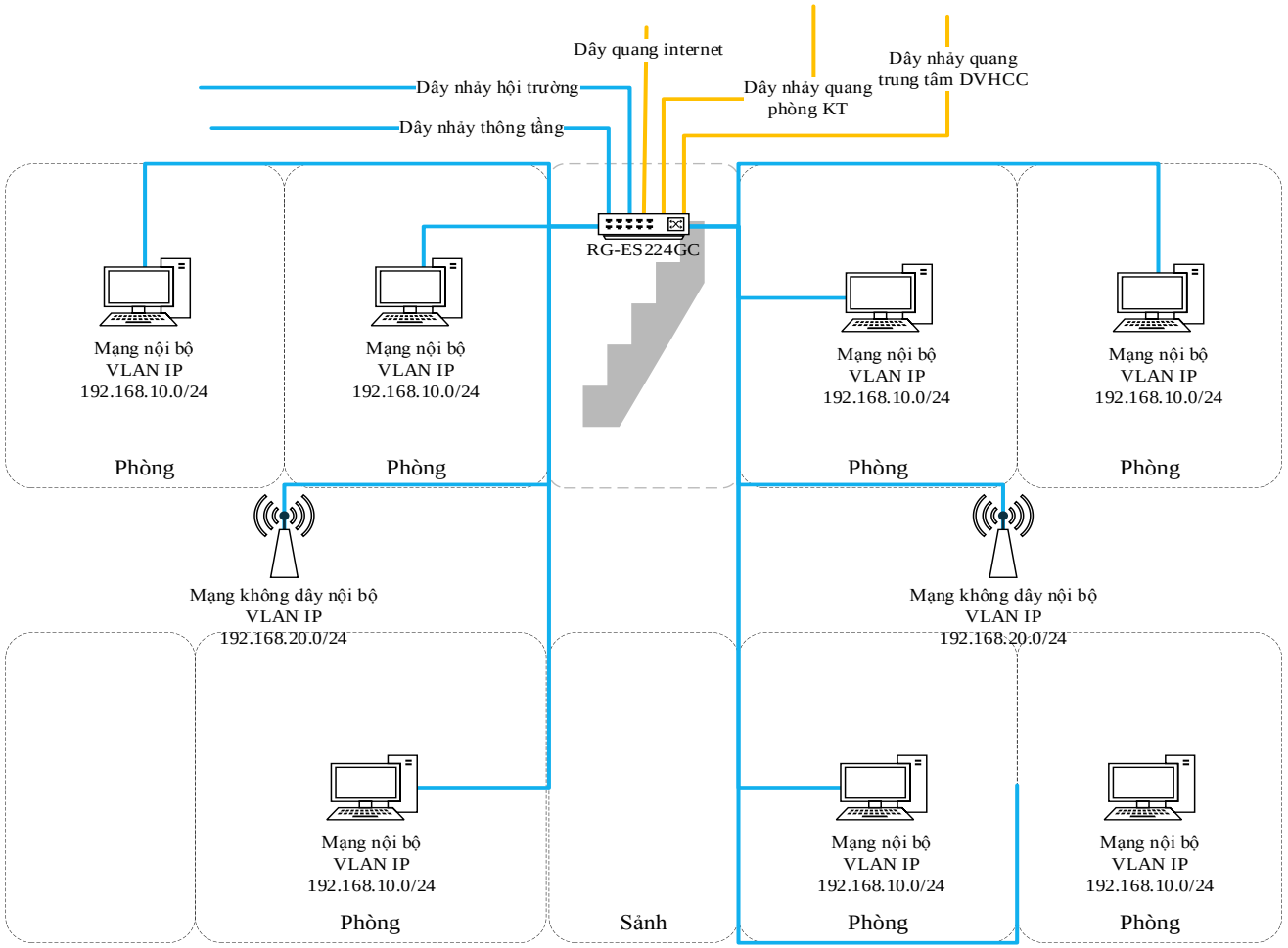
+ Vùng mạng máy chủ: (Đơn vị không trang bị và sử dụng máy chủ)

b) Mô hình sơ đồ vật lý hệ thống

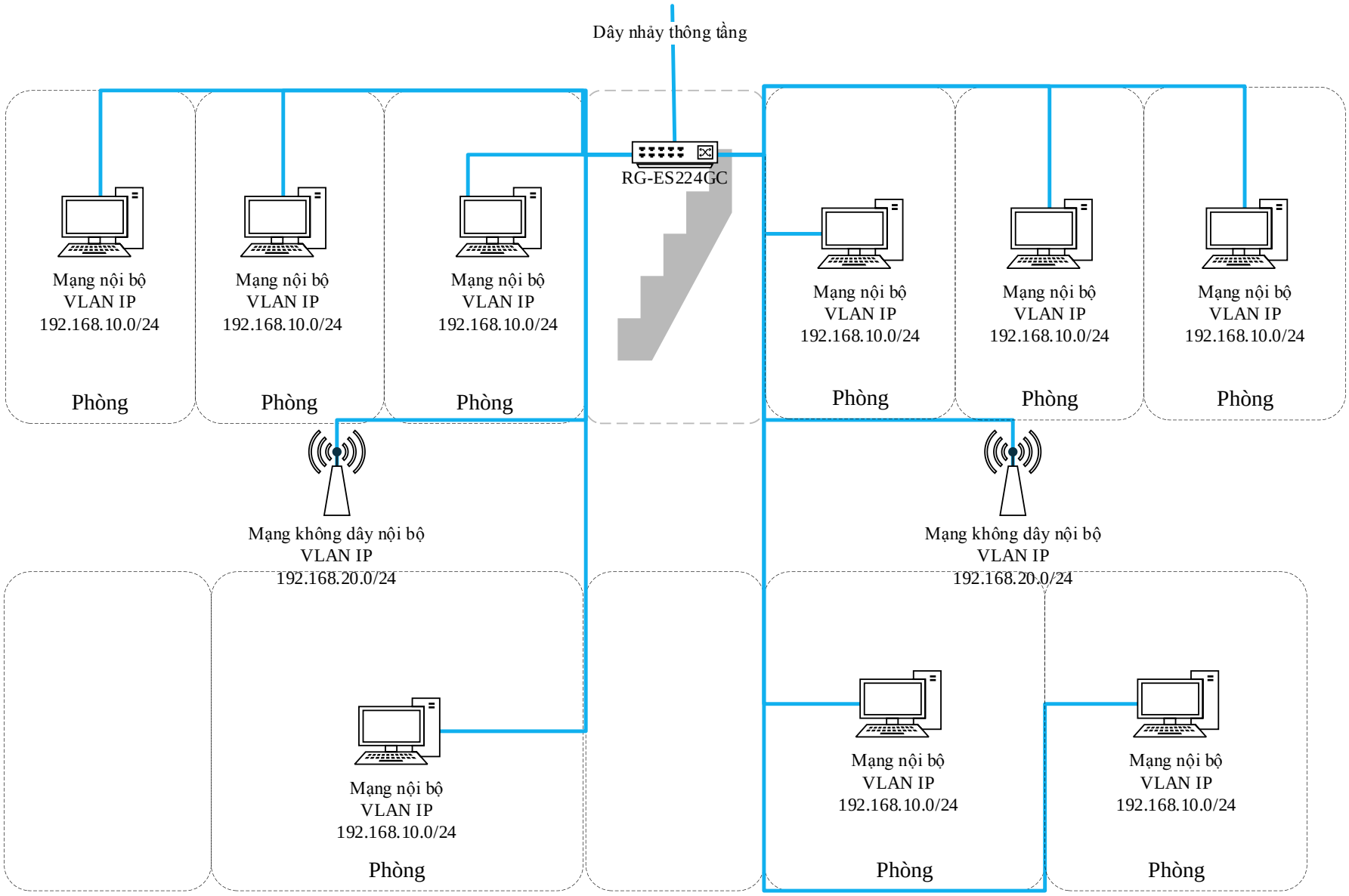


Hình 2. Sơ đồ vật lý của hệ thống

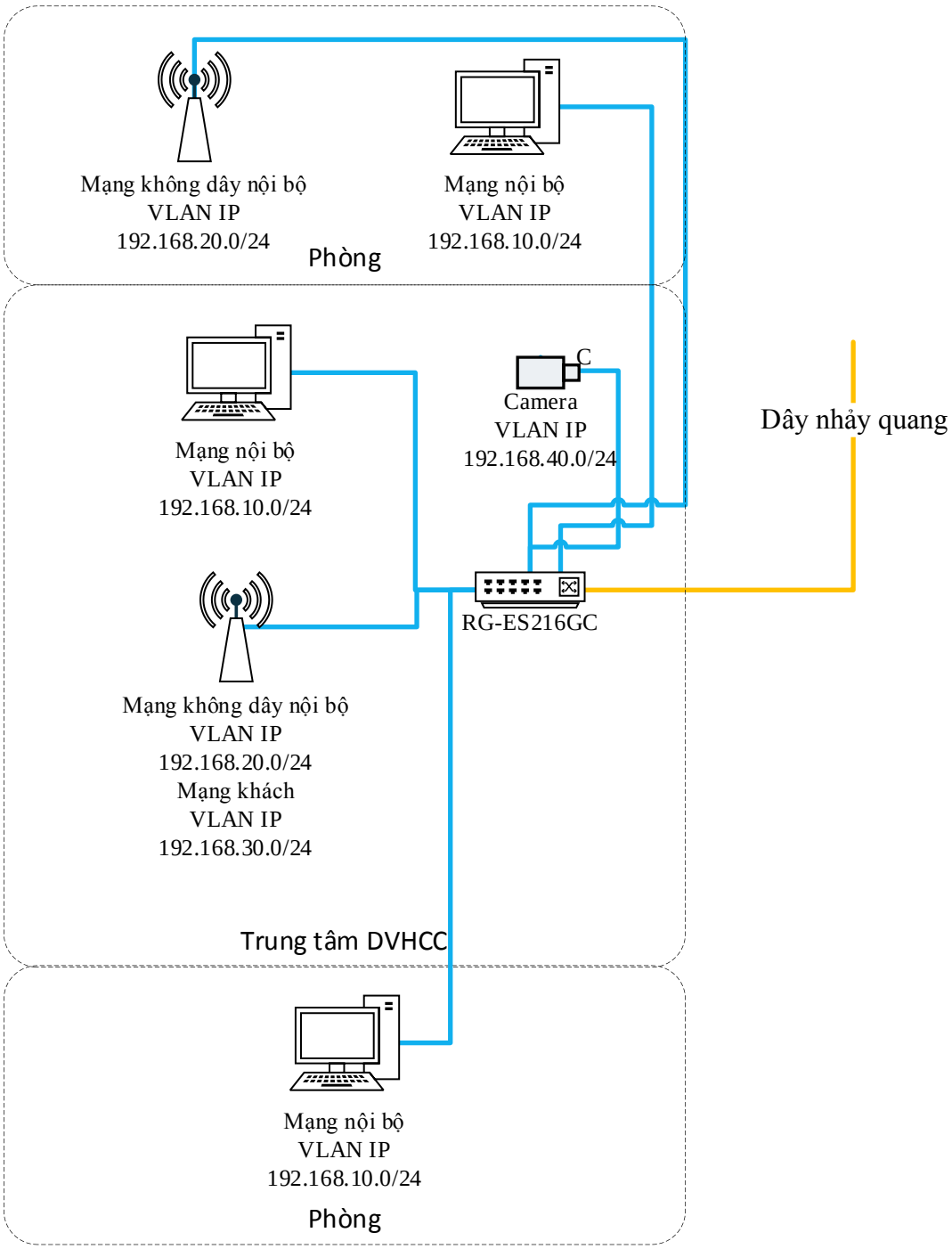
4.2. Sơ đồ mặt bằng



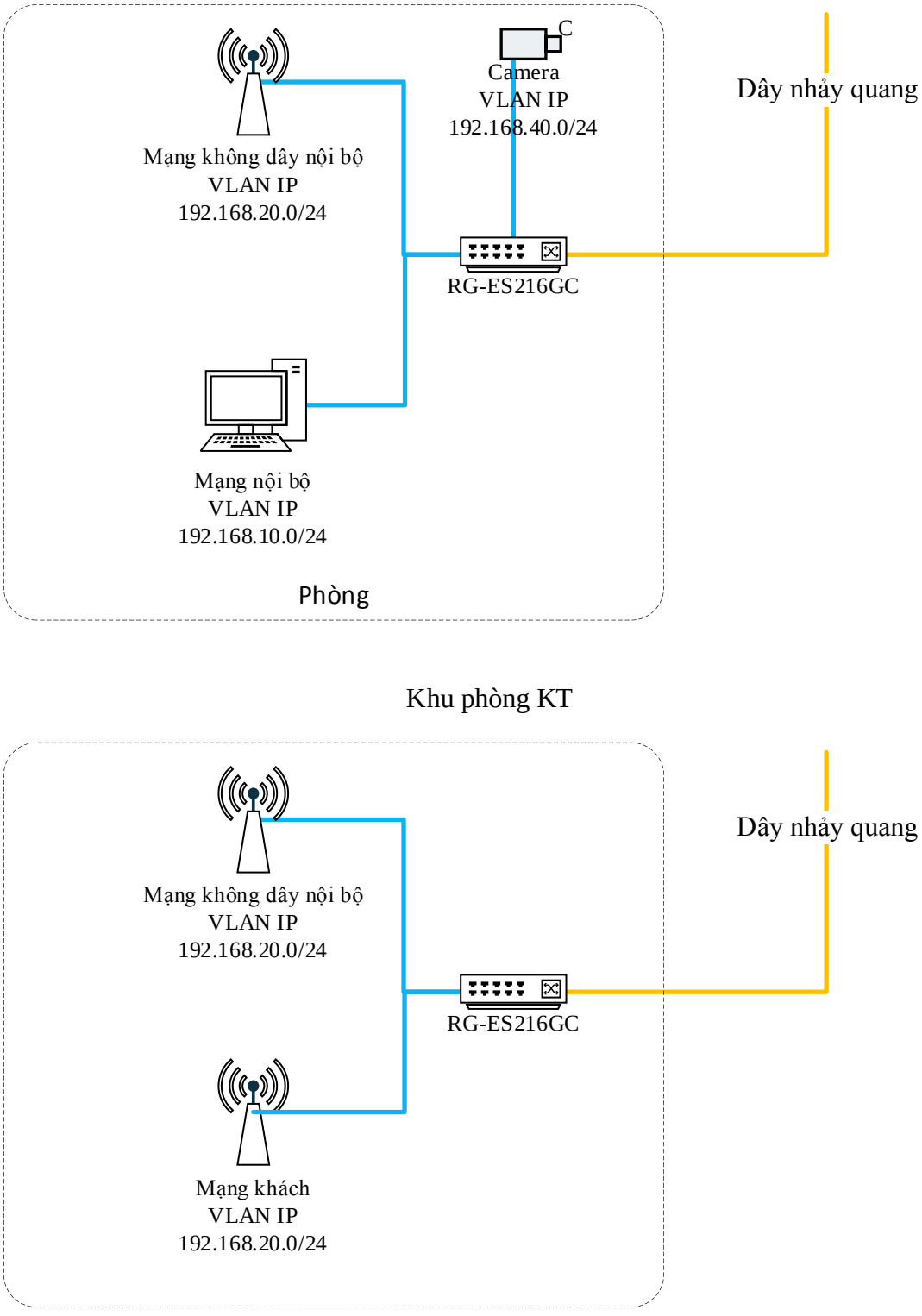
Tòa UBND - Tầng 1



Tòa UBND - Tầng 2



Khu trung tâm DVHCCC



Hình 3. Sơ đồ mặt bằng hệ thống thông tin UBND Xã Đăk Plô

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 Router của ISP
2	Modem Viettel	Vùng mạng biên	Kết nối và định tuyến động với Router của ISP
3	Router/ MikroTik CCR2004-16G-2S+	Vùng mạng biên	Kết nối, định tuyến cân bằng tải hai nhà mạng khác nhau. Kết nối vùng mạng công dân
4	Firewall/ Sophos XGS 2100 HW	Vùng mạng biên	Thiết bị Firewall thiết lập để quản lý, kiểm soát truy cập vào/ra giữa các vùng mạng. Thiết bị truy nhập kết nối trực tiếp người dùng cuối, phân tách lưu lượng bằng VLAN, hỗ trợ QoS và bảo mật cơ bản, đồng thời liên kết lên các lớp mạng trên.
5	Switch/ Ruijie Reyee RG-ES224GC	Vùng mạng nội bộ	Thiết bị truy nhập kết nối trực tiếp người dùng cuối.
6	Switch/ Ruijie Reyee RG-ES216GC	Vùng mạng nội bộ	Thiết bị truy nhập kết nối trực tiếp người dùng cuối
7	Switch/ Ruijie Reyee RG-ES208GC	Vùng mạng nội bộ	Thiết bị truy nhập kết nối trực tiếp người dùng cuối

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 đặt/ Vùng mạng/ HĐH	Mục đích sử dụng
1	Hệ thống quản lý văn bản điều hành iOffice	UBND tỉnh Thuê hệ thống tại đơn vị cung cấp dịch vụ, cấp quyền và tài khoản cho UBND xã sử dụng	Quản lý toàn bộ nghiệp vụ xử lý văn bản UBND. Hệ thống đã được thuyết minh đảm bảo an toàn

			thông tin cấp độ 3 theo quy định.
2	Hệ thống thông tin giải quyết thủ tục hành chính	UBND tỉnh Thuê hệ thống tại đơn vị cung cấp dịch vụ, cấp quyền và tài khoản cho UBND xã sử dụng	Quản lý toàn bộ nghiệp vụ cung cấp dịch vụ công cho công dân. Hệ thống đã được thuyết minh đảm bảo an toàn thông tin cấp độ 3 theo quy định.
3	Hệ thống quản lý cán bộ công chức viên chức	Sở Nội vụ tỉnh QN Thuê hệ thống tại đơn vị cung cấp dịch vụ, cấp quyền và tài khoản cho UBND xã sử dụng	Quản lý công chức viên chức của UBND. Hệ thống đã được thuyết minh đảm bảo an toàn thông tin cấp độ 3 theo quy định.
4	Hệ thống thông tin báo cáo tỉnh	UBND tỉnh Thuê hệ thống tại đơn vị cung cấp dịch vụ, cấp quyền và tài khoản cho UBND xã sử dụng	Quản lý báo cáo bộ ngành địa phương của UBND. Hệ thống đã được thuyết minh đảm bảo an toàn thông tin cấp độ 3 theo quy định.
5	Hệ thống thư điện tử công vụ	UBND tỉnh cung cấp dịch vụ, cấp quyền và tài khoản cho UBND xã sử dụng	Quản lý thư điện tử công vụ. Hệ thống đã được thuyết minh đảm bảo an toàn thông tin cấp độ 3 theo quy định.
6	Hệ thống Cổng thông tin điện tử	UBND tỉnh Thuê hệ thống tại đơn vị cung cấp dịch vụ, cấp quyền và tài khoản cho UBND xã sử dụng	Quản lý cổng thông tin điện tử của UBND. Hệ thống đã được thuyết minh đảm bảo an toàn

			thông tin cấp độ 2 theo quy định.

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

4.5. Thống kê hệ thống thiết bị

STT	Khu vực	PC&Laptop
1	Tòa UBND - Tầng 1	15
2	Tòa UBND - Tầng 2	15
3	Trung tâm DVHCC	9
4	Phòng Kinh tế	5
Tổng		**51**

Bảng 3. Bảng thống kê hệ thống thiết bị trong hệ thống

Danh mục phần mềm, ứng dụng được phép sử dụng trên máy tính của UBND Xã Đăk Plô bao gồm:

STT	Phần mềm/Ứng dụng	Bản quyền
1	Phần mềm trình duyệt web: Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, Cốc Cốc;	Bản miễn phí
2	Các phiên bản phần mềm Microsoft Office 2013, 2016, 2019, 2021, 2024	Bản kích hoạt trực tuyến
3	Zoom Meeting	Bản miễn phí
4	Hệ điều hành Microsoft Windows 8 trở lên bao gồm Windows 8, Windows 8.1, Windows 10 và Windows 11	Bản kích hoạt trực tuyến

Bảng 4. Bảng phần mềm, ứng dụng được phép sử dụng

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

STT	Vùng mạng	IP Private	Ghi chú
1	Vùng mạng biên		IP Public động do nhà mạng (ISP VNPT và Viettel) cấp phát

2	Vùng mạng nội bộ	192.168.10.0/24	Cấu hình sau khi mua sắm bổ sung các thiết bị
3	Vùng mạng không dây nội bộ	192.168.20.0/24	Cấu hình sau khi mua sắm bổ sung các thiết bị
4	Vùng mạng khách	192.168.30.0/24	Cấu hình sau khi mua sắm bổ sung các thiết bị
5	Vùng camera an ninh	192.168.40.0/24	Cấu hình sau khi mua sắm bổ sung các thiết bị
6	Vùng máy chủ	192.168.50.0/24	Không sử dụng
7	Vùng DMZ	192.168.60.0/24	Cấu hình sau khi mua sắm bổ sung các thiết bị

Bảng 5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

4.7. Tủ thiết bị mạng của hệ thống thông tin

- Hệ thống thông tin của Ủy ban nhân dân xã Đăk Plô đã được bố trí tủ thiết bị mạng (tủ rack) để lắp đặt, quản lý và bảo vệ các thiết bị hạ tầng công nghệ thông tin. Tủ thiết bị mạng được sử dụng nhằm đảm bảo việc sắp xếp thiết bị khoa học, thuận tiện cho công tác quản trị, vận hành và bảo trì hệ thống, đồng thời hạn chế các tác động vật lý có thể ảnh hưởng đến an toàn của thiết bị.

- Tủ thiết bị mạng có kích thước phù hợp với quy mô hệ thống (từ 6U đến 12U), được thiết kế dạng tủ treo tường hoặc tủ đứng, có cửa khóa bảo vệ và hệ thống thông gió. Tủ được đặt tại vị trí an toàn trong khu vực làm việc của đơn vị, bảo đảm các điều kiện về nguồn điện, nhiệt độ môi trường, độ thông thoáng và hạn chế tiếp cận của người không có nhiệm vụ.

4.8. Phòng đặt thiết bị của hệ thống thông tin

- Hệ thống mạng nội bộ tại UBND, HĐND xã Đăk Plô không trang bị các máy chủ ứng dụng, thiết bị tủ mạng tương đối nhỏ gọn. Không cần thiết trang bị phòng đặt thiết bị riêng mà sử dụng chung với phòng làm việc của cán bộ, công chức viên chức tại đơn vị.

PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

Hệ thống thông tin UBND Xã Đăk Plô 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 UBND Xã Đăk Plô	2	Khoản 1 Điều 8 Nghị định số 85/2016/NĐ- CP

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

Hệ thống mạng nội bộ Ủy ban nhân dân, Hội đồng nhân dân xã Đăk Plô là hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan và có xử lý thông tin riêng, thông tin cá nhân của người sử dụng nhưng không xử lý thông tin bí mật nhà nước. Căn cứ theo Khoản 1 Điều 8 Nghị định số 85/2016/NĐ-CP, hệ thống này được đề xuất xác định ở cấp độ 2 về an toàn hệ thống thông tin.

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

- Chính sách an toàn thông tin
- Xây dựng và công bố
- Rà soát, sửa đổi

2. Tổ chức bảo đảm an toàn thông tin

- Đơn vị chuyên trách về an toàn thông tin
- Phối hợp với cơ quan/ tổ chức có thẩm quyền

3. Bảo đảm nguồn nhân lực

- Tuyển dụng
- Trong quá trình làm việc
- Chấm dứt hoặc thay đổi công việc

4. Quản lý thiết kế, xây dựng hệ thống

- Thiết kế an toàn hệ thống thông tin
- Phát triển phần mềm thuê khoán
- Thử nghiệm và nghiệm thu hệ thống

5. Quản lý vận hành hệ thống

- Quản lý an toàn mạng
- Quản lý an toàn máy chủ và ứng dụng
- Quản lý an toàn dữ liệu
- Quản lý sự cố an toàn thông tin
- Quản lý an toàn người sử dụng đầu cuối

6. **Phương án Quản lý rủi ro an toàn thông tin**

7. **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 đề xuất cấp độ 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. Kiểm soát truy cập từ bên trong mạng

1.4. Nhật ký hệ thống

1.5. Phòng chống xâm nhập

1.6. Bảo vệ thiết bị hệ thống

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

2.2. Kiểm soát truy cập

2.3. Nhật ký hệ thống

2.4. Phòng chống xâm nhập

2.5. Phòng chống phần mềm độc hại

2.6. Xử lý máy chủ khi chuyển giao

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

3.2. Kiểm soát truy cập

3.3. Nhật ký hệ thống

3.4. An toàn ứng dụng và mã nguồn

4. Bảo đảm an toàn dữ liệu

4.1. Bảo mật dữ liệu

4.2. Sao lưu dự phòng

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 06 tháng, kể từ khi hồ sơ đề xuất cấp độ được phê duyệt.

Thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống thông tin UBND Xã Đăk Plô 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	2	Phụ lục I
2	Thuyết minh phương án đáp ứng yêu cầu kỹ thuật đối với Hệ thống thông tin UBND Xã Đăk Plô	2	Phụ lục II

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

1. Thiết lập chính sách an toàn thông tin

1.1. Chính sách an toàn thông tin

Yêu cầu	Xây dựng chính sách an toàn thông tin gồm: - Quản lý an toàn mạng - Quản lý an toàn máy chủ và ứng dụng - Quản lý an toàn dữ liệu - Quản lý an toàn người sử dụng đầu cuối
Hiện trạng	Đáp ứng. - Tham chiếu tại Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi. - Tham chiếu tại Điều 8, Điều 13, Điều 14 và Điều 15, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Xây dựng chính sách an toàn thông tin 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 thông tin 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. d) Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống. e) Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: - Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như USB hoặc cloud.

	- Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. g) Truy cập và quản lý cấu hình hệ thống: - Cấu hình hệ thống tư xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN. - Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN. - Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập. **2. Quản lý an toàn máy chủ và ứng dụng** a) Hệ thống thông tin 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 thông tin phải được bảo vệ bằng tường lửa 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. d) Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống. g) Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần. e) Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc. h) Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống. i) Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: - Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như USB hoặc cloud. - Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. k. Truy cập và quản lý cấu hình hệ thống: - Cấu hình hệ thống tư xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN.

	- Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN. - Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập. **3. Quản lý an toàn dữ liệu** a) Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn. b) 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 ATTT mạng xảy ra. c) 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. d) Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ. g) 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. h) 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. i) 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. k) Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ, phương tiện lưu trữ. **4. Quản lý an toàn người sử dụng đầu cuối** a) Quản lý truy cập, sử dụng tài nguyên nội bộ - Người sử dụng khi truy cập, sử dụng tài nguyên phải tuân thủ các quy định của pháp luật về bảo đảm ATTT và các quy định của cơ quan, tổ chức. - Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn, quy trình dưới sự giám sát của bộ phận chuyên trách về ATTT.

	- Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống. b) Quản lý truy cập mạng và tài nguyên trên Internet - Người sử dụng khi truy cập, sử dụng Internet phải tuân thủ các quy định của pháp luật về bảo đảm ATTT và các quy định của cơ quan, tổ chức. - Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn, quy trình dưới sự giám sát của quản trị viên hệ thống. - Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống. c) Cài đặt và sử dụng máy tính an toàn - Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về ATTT mạng. Chịu trách nhiệm bảo đảm ATTT mạng trong phạm vi trách nhiệm và quyền hạn được giao. - Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng. - Khi phát hiện nguy cơ hoặc sự cố mất ATTT mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách CNTT của cơ quan, đơn vị để kịp thời ngăn chặn, xử lý. - Tham gia các chương trình đào tạo, hội nghị về ATTT mạng được cơ quan chức năng, đơn vị chuyên môn tổ chức.

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. Tham chiếu tại Điều 24, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Quy chế này được tổ chức/bộ phận trình người đứng đầu đơn vị vận hành trước khi công bố áp dụng.

1.3. Rà soát, sửa đổi

Yêu cầu	Định kỳ 03 năm hoặc khi có thay đổi 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 tại Điều 28, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Rà soát, sửa đổi: 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. Có hồ sơ lưu lại thông tin phản hồi của đối tượng áp dụng chính sách trong quá trình triển khai, áp dụng chính sách an toàn thông tin.

2. Tổ chức bảo đảm an toàn thông tin

2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Có bộ phận có trách nhiệm bảo đảm an toàn thông tin cho tổ chức.
Hiện trạng	Đáp ứng. Tham chiếu của UBND tỉnh về việc phân công đơn vị chuyên trách an toàn thông tin mạng của UBND tỉnh Quảng Ngãi.
Phương án	Trong cơ cấu tổ chức và phân công nhiệm vụ, đơn vị chuyên trách về an toàn thông tin tại tỉnh Quảng Ngãi là Công an tỉnh Quảng Ngãi (phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao). Tại UBND xã có phân công cán bộ công chức là thành viên đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi, thực hiện các công tác đảm bảo an toàn thông tin cho tổ chức.

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

Yêu cầu	- Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin. - 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; - Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.
Hiện trạng	Đáp ứng. - Tham chiếu Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi. - Tham chiếu Điều 5, 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
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: UBND giao Văn phòng HĐND và UBND là đầu mối liên hệ, phối hợp các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho hệ thống thông tin UBND xã Đăk Plô. 2. 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) Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi: - Đại úy Phạm Nhật Trí – Cán bộ Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh; số điện thoại: 0966 833 937. - Thượng úy Hoàng Gia Bảo - Cán bộ Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh; số điện thoại: 0964 634 357. b) Trung tâm An ninh mạng Quốc gia – Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an

	- Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT) - Số điện thoại: 0590 505 268 - Email: vncert@nca.gov.vn 3. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền. UBND hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

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. - Tham chiếu Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi. - Tham chiếu Khoản 1 Điều 6, 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ: Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.

3.2. Trong quá trình làm việc

Yêu cầu	- Có quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc; -Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng

Hiện trạng	Đáp ứng. - Tham chiếu Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi. - Tham chiếu Khoản 2 Điều 6, Quyết định 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	1. Quy định về việc thực bảo đảm an toàn thông tin trong quá trình làm việc: a) Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển trung cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin. b) Cán bộ chuyên trách phải tổ chức quản lý định doanh đối với tất cả người sử dụng tham gia gia sử dụng hệ thống thông tin. c) Các bộ phận, cá nhân tham gia sử dụng dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh mạng và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp. d) Tài khoản quản trị hệ thống (mạng, hệ điều hành, thiết bị kết nối mạng, phần mềm, ứng dụng, cơ sở dữ liệu…) phải tách biệt với tài khoản truy cập của người sử dụng thông thường. Tài khoản quản trị hệ thống phải giao đích danh cá nhân làm quản công tác quản trị. Phân quyền sử dụng tài khoản quản trị theo chức năng nhiệm vụ của cá nhân trong công tác vận hành quản trị hệ thống. 2. Với người sử dụng: a) 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. b) Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT. c) Chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp chức năng, trách nhiệm, quyền hạn của mình; không truy cập, mở các trang tin, thư điện tử không rõ nguồn gốc.

	d) Có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu với người khác. Đặt mật khẩu với 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 trên thiết bị. e) Khóa máy tính khi tạm thời rời nơi đặt máy tính; tắt máy tính khi rời khỏi cơ quan. g) Phải 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. 2. 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 chức 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. - Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.
Hiện trạng	Đáp ứng. - Tham chiếu Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi. - Tham chiếu Khoản 3 Điều 6, Quyết định 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	1. 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. 2. Bộ phận chuyên trách thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

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

4.1. Thiết kế an toàn hệ thống thông tin

Yêu cầu	- Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin. - Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin. - Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ. - Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin - Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.
Hiện trạng	Đáp ứng. Tham chiếu tại Điều 9, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Quy định về thiết kế an toàn hệ thống thông tin. 1. Đơn vị thiết kế, xây dựng HTTT phải cung cấp tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành HTTT: - Tài liệu phân tích lựa chọn kiến trúc, công nghệ; - Tài liệu thiết kế tổng thể hệ thống thể hiện thiết kế hạ tầng và kết nối các thành phần của hệ thống; - Các giải pháp, thiết bị của HTTT đáp ứng các quy định của Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn HTTT theo cấp độ (Thông tư số 12/2022/TT-BTTTT). 2. Đơn vị thiết kế, xây dựng HTTT phải cung cấp các tài liệu "Kiến trúc hệ thống" trong đó có mô tả thiết kế và các thành phần của HTTT thông qua một số mô hình kiến trúc khác nhau nhằm miêu tả hệ thống dưới nhiều góc nhìn khác nhau, bao gồm: - Thiết kế kiến trúc ứng dụng; - Thiết kế kiến trúc dữ liệu;

	- Thiết kế kiến trúc vật lý. 3. Đơn vị thiết kế, xây dựng HTTT phải cung cấp tài liệu mô tả phương án bảo đảm ATTT theo cấp độ được quy định tại Thông tư số 12/2022/TT-BTTTT. 4. Đơn vị thiết kế, xây dựng HTTT phải cung cấp tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm ATTT, trong đó cần đảm bảo các tiêu chí: - Đảm bảo có từ 2 - 3 công nghệ được phân tích và đưa ra phương án lựa chọn; - Phân tích các ưu, nhược điểm của từng công nghệ để từ đó chọn ra công nghệ áp dụng phù hợp nhất. 5. Khi có thay đổi thiết kế, cần đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống. Khi có thay đổi thiết kế, đơn vị thiết kế, xây dựng HTTT, cần phối hợp với các đơn vị liên quan đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, xây dựng kế hoạch trước khi có thay đổi, kèm theo các tài liệu sau: - Căn cứ thực hiện thay đổi (công văn, tờ trình); - Kế hoạch chi tiết các bước thực hiện. 6. Phương án quản lý và bảo vệ hồ sơ thiết kế Hồ sơ thiết kế được sắp xếp một cách khoa học để dễ quản lý, dễ nộp lưu và dễ tìm khi cần. Hồ sơ thiết kế được giữ gìn bí mật, bảo quản theo chế độ tài liệu mật, không được mang hồ sơ thiết kế ra khỏi cơ quan hoặc tùy tiện cung cấp hồ sơ thiết kế cho cá nhân, đơn vị khác.

4.2. Phát triển phần mềm thuê khoán

Yêu cầu	- Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán - Yêu cầu các nhà phát triển cung cấp mã nguồn mở phần mềm
Hiện trạng	Đáp ứng. Tham chiếu Điều 10, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.

Phương án	Quy định đối với việc phát triển phần mềm thuê khoán: 1. Đối với các nội dung liên quan đến việc phát triển phần mềm, đơn vị được thuê khoán phải đảm bảo có các tài liệu sau: - Biên bản làm việc. - Biên bản thống nhất nội dung công việc. - Hợp đồng giữa các đơn vị. - Hồ sơ liên quan đến ATTT, bảo mật của phần mềm, cơ sở dữ liệu; các cam kết đảm bảo ATTT, an ninh mạng. 2. Nhà phát triển phần mềm phải cung cấp mã nguồn sản phẩm cho đơn vị xây dựng phần mềm theo hình thức ghi đĩa DVD hoặc USB; yêu cầu tệp trên DVD, USB cần phải đặt mật khẩu để đảm bảo ATTT - Mã nguồn đã được nhà phát triển tự đánh giá và có biên bản kiểm thử, đánh giá Đạt trước khi bàn giao cho đơn vị thuê. - Phối hợp với đơn vị chủ quản HTTT đánh giá mã nguồn và có phương án xử lý lỗi (nếu có). 3. Kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng Đơn vị thuê và đơn vị phát triển phối hợp thực hiện kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng: - Mã nguồn phải được đánh giá ATTT trước khi đưa vào môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng. - Tất cả các lỗi liên quan đến mã nguồn (nếu có) sau khi được khắc phục, phải được đánh giá ATTT và có biên bản đánh giá trước khi đưa vào sử dụng. 4. Kiểm tra, đánh giá ATTT, trước khi đưa vào sử dụng Hệ thống được đầu tư phải được kiểm định ATTT trước khi đưa vào vận hành khai thác: - Kiểm tra hệ thống, mã nguồn có các lỗ hổng bảo mật không. Thực hiện cập nhật các bản vá ATTT hoặc nâng cấp lên phiên bản mới nhất của hãng để đảm bảo vá hoàn toàn các lỗ hổng bảo mật. - Thực hiện nâng cấp, xử lý điểm yếu ATTT của thiết bị hệ thống trước khi đưa vào sử dụng. - Máy chủ phải được cài đặt hệ điều hành, phần mềm, phần mềm diệt virus có bản quyền.

	5. Kiểm tra, đánh giá ATTT cho phần mềm khi thay đổi mã nguồn, kiến trúc phần mềm Khi có thay đổi thiết kế, đơn vị thuê và đơn vị phát triển phần mềm phối hợp đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống, cần xây dựng kế hoạch trước khi có thay đổi bao gồm tối thiểu các tài liệu sau: - Căn cứ thực hiện thay đổi (công văn, tờ trình); - Kế hoạch chi tiết các bước thực hiện. 6. Cam kết đảm bảo tính bí mật của mã nguồn và bản quyền của phần mềm phát triển: - Bên phát triển phải có cam kết về bảo đảm tính bí mật của mã nguồn, không cung cấp cho tổ chức hoặc cá nhân khác. - Bên phát triển có cam kết không có tranh chấp về bản quyền phát triển của phần mềm. - Các cá nhân tham gia phát triển, triển khai HTTT phải ký biên bản cam kết bảo mật ATTT.

4.3. Thử nghiệm và nghiệm thu hệ thống

Yêu cầu	- Thực hiện kiểm thử hệ thống trước khi đi vào vận hành, khai thác sử dụng hệ thống - Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng. - Tham chiếu Điều 11, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Thử nghiệm và nghiệm thu hệ thống: 1. Thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng. Các sản phẩm, thiết bị được đầu tư trong hệ thống phải được kiểm định ATTT trước khi đưa vào vận hành khai thác: - Kiểm tra phiên bản phần mềm cho phần cứng (firmware) các thiết bị mạng quan trọng như: Tường lửa, Switch, IDS/IPS,... có lỗ hổng bảo mật không. Thực hiện cập nhật các bản vá hoặc nâng cấp lên phiên bản mới nhất của hãng để đảm bảo ATTT.

	- Các thiết bị hệ thống trước khi được đưa vào sử dụng phải được qua kiểm định về an ninh, an toàn, cháy nổ theo quy định của các cơ quan chức năng; thực hiện nâng cấp, xử lý điểm yếu ATTT trước khi đưa vào sử dụng. - Đảm bảo máy chủ không chứa mã độc; thực hiện gỡ bỏ các hệ điều hành cũ đối với máy chủ và thực hiện xóa dữ liệu (Format) đối với các ổ cứng trước khi đưa vào sử dụng. 2. Nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống. a) Hệ thống được thử nghiệm tổng thể trước khi đưa vào sử dụng và định kỳ hàng năm để đảm bảo tính an toàn, thống nhất của hệ thống. b) Nội dung, kế hoạch và quy trình nghiệm thu hệ thống được thực hiện theo Thông tư số 16/2024/TT-BTTTT ngày 30 tháng 12 năm 2024 của Bộ trưởng Bộ Thông tin và Truyền thông. 3. Cơ quan có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống Đơn vị vận hành đảm nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống như sau: - Kiểm thử, nghiệm thu chức năng của hệ thống. - Kiểm thử, nghiệm thu bảo đảm ATTT. - Kiểm thử, nghiệm thu hệ thống nội bộ của đơn vị phát triển. 4. Đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống. 5. Báo cáo nghiệm thu được ký xác nhận của Ủy ban nhân dân xã Đăk Plô trước khi đưa vào sử dụng.

5. Quản lý vận hành hệ thống thông tin

5.1. Quản lý an toàn mạng

Chính sách, quy trình quản lý an toàn máy chủ gồm:

Yêu cầu	- Quản lý, vận hành hoạt động bình thường của hệ thống - Cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố - Truy cập và quản lý cấu hình hệ thống
Hiện trạng	Đáp ứng.

	- Tham chiếu Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi. - Tham chiếu Điều 11, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	**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, rui ro và duy trì an toàn cho các máy tính, ứng dụng sử dụng mạng: - Có sở đồ logic và vật lý về hệ thống mạng, 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. - Sử dụng thiết bị tường lửa, thiết bị phát hiện và kiểm soát truy từ bên ngoài mạng và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng; Kiểm soát truy cập từ bên trong mạng; kết nối hệ thống giám sát tập trung (nếu có); 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 trung 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 cáp. 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 công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn. **2. Cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố** a) Định kỳ hàng tháng hoặc khi có thay đổi cấu hình trên hệ thống, bộ phận chuyên trách thực hiện quy trình sao lưu dự

	phòng được sao lưu thông qua hệ thống sao lưu dữ liệu. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập. b) Các dữ liệu yêu cầu sao lưu, dự phòng gồm: 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. Truy cập và quản lý cấu hình hệ thống** a) Cán bộ quản lý, 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, vận hành có trách nhiệm theo dõi và phát hiện các trường hợp trung cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho Bộ phận chuyên trách an toàn, an ninh mạng UBND xã Đăk Plô để tiến hành ngăn chặn, thu hội, khóa quyền truy cập của các tài khoản vi phạm. c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) 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.

5.2. Quản lý an toàn máy chủ và ứng dụng

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

Yêu cầu	- Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ. - Truy cập mạng của máy chủ. - Truy cập và quản trị máy chủ và ứng dụng. - Cập nhật; sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.
Hiện trạng	Đáp ứng. - Tham chiếu Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin

	trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi. - Tham chiếu Điều 13, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm: **1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ** a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tụ, ổn định và an toàn b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện xử lý những sự cố nếu có. c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm. - Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp. - Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không có nhu cầu sử dụng….. - Các bản quyền phần mềm cần được thống kê, quản lý thời gian, hạn để phục vụ cho việc gia hạn. **2. Truy cập mạng của máy chủ** a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành. c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet của trang thông tin điện tử, dịch vụ công, thư điện tử…; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet. **3. Truy cập và quản trị máy chủ và ứng dụng.** a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.

	b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành. c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet. **4. Cập nhật; sao lưu dự phòng và khôi phục sau khi xảy ra sự cố** Triển khai hệ thống phương tiện lưu trữ độc lập với hệ thống thông lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được sao lưu theo từng loại, nhóm thông tin gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: Tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

5.3. Quản lý an toàn dữ liệu

Chính sách, quy trình quản lý an toàn dữ liệu bao gồm:

Yêu cầu	- Chính sách, quy trình dự phòng và khôi phục dữ liệu - 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.
Hiện trạng	Đáp ứng. - Tham chiếu Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi. - Tham chiếu Điều 14, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Chính sách, quy trình quản lý an toàn dữ liệu bao gồm:

	1. Chính sách, quy trình dự phòng và khôi phục dữ liệu: 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, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian 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: Bộ phận chuyên trách an toàn thông tin, an ninh mạng của UBND xã Đăk Plô 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. 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 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 phê duyệt. 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.

5.4. Quản lý sự cố an toàn thông tin

Chính sách, quy trình quản lý sự cố an toàn thông tin bao gồm:

Yêu cầu	- Phân nhóm sự cố an toàn thông tin mạng - Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng. - Kế hoạch ứng phó sự cố an toàn thông tin mạng; - Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin. - Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường.

<table>
<tr><td></td><td>-Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng.
- Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin.</td></tr>
<tr><td>Hiện trạng</td><td>Đáp ứng.
- Tham chiếu Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi.
- Đã quy định tại Điều 15, Quyết định 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.</td></tr>
<tr><td>Phương án</td><td>Chính sách, quy trình quản lý sự cố an toàn thông tin bao gồm:
1. Quy định về phân nhóm sự cố an toàn thông tin mạng
Sự cố ATTT được phân loại theo hình thức bao gồm:
- Sự cố do Tấn công từ chối dịch vụ
- Sự cố do Mã độc, phần mềm độc hại
- Sự cố do Truy cập trái phép
- Sự cố do Vi phạm chính sách, Rò rỉ dữ liệu
- Sự cố do Khai thác và thu thập thông tin trái phép (Hacking)
- Sự cố do tấn công kỹ thuật
Mức độ sự cố phân loại theo mức độ ảnh hưởng và cấp độ hệ thống thông tin:
- M1: Sự cố Nghiêm trọng
- M2: Sự cố Lớn
- M3: Sự cố Thông thường
Mức độ nghiêm trọng của sự cố ATTT được xác định trên cơ sở tổng hợp Cấp độ hệ thống và Mức độ ảnh hưởng theo bảng sau:
<table>
<tr><td rowspan="2">Mức độ ảnh hưởng</td><td colspan="5">Cấp độ hệ thống</td></tr>
<tr><td>Cấp 1</td><td>Cấp 2</td><td>Cấp 3</td><td>Cấp 4</td><td>Cấp 5</td></tr>
<tr><td>Nghiêm trọng</td><td>M3</td><td>M2</td><td>M1</td><td>M1</td><td>M1</td></tr>
</table>
</td></tr>
</table>

Lớn	**M3**	**M2**	**M2**	**M2**	**M1**
Thông thường	**M3**	**M3**	**M3**	**M2**	**M2**

2. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu và kế hoạch ứng phó sự cố an toàn thông tin mạng

- Ghi nhận, tiếp nhận thông báo, báo cáo sự cố an toàn thông tin mạng theo đúng quy trình.
- Thông báo ngay thông tin sự cố đến Bộ phận chuyên trách an toàn, an ninh mạng của UBND.
- Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo Công an tỉnh; đề xuất, xin ý kiến chỉ đạo trong trường hợp không thuộc thẩm quyền, phạm vi trách nhiệm của mình hoặc vượt khả năng xử lý.

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

3.1 Văn phòng HĐND và UBND chịu trách nhiệm:

a) Thực hiện theo dõi giám sát ATTT, ANM 24/7, tổng hợp thông tin dữ liệu;

b) Tổ chức, điều phối ứng cứu, xử lý, khắc phục khẩn cấp 24/7 các cuộc tấn công, sự cố ATTT, ANM;

3.2. Toàn thể các khoa, phòng chuyên môn và đơn vị chức năng trực thuộc, cùng với đội ngũ cán bộ, viên chức và người lao động đang công tác tại UBND xã Đăk Plô có trách nhiệm thông báo kịp thời tới Bộ phận chuyên trách an toàn thông tin, an ninh mạng của UBND chịu trách nhiệm ứng cứu và xử lý sự cố an toàn hệ thống thông tin khi gặp các sự kiện an toàn hệ thống thông tin bao gồm các tình huống sau:

a) Các lỗi, trục trặc trong hoạt động của phần mềm hoặc phần cứng;

b) Các tình huống vi phạm các quy định, quy tắc an toàn;

c) Các xâm nhập vào khu vực làm việc, khu vực an ninh trái phép;

d) Các thay đổi trên hệ thống không được cảnh báo hoặc lên kế hoạch;

đ) Các truy cập vào hệ thống trái phép;

e) Các tình huống bị lộ thông tin mức độ mật trở lên;

f) Các điểm yếu, lỗ hổng bảo mật trên các hệ thống thông tin có khả năng bị tấn công khai thác.

3.3. Cán bộ chịu trách nhiệm ứng cứu và xử lý sự cố an toàn hệ thống thông tin phải xem xét đánh giá các sự kiện an toàn hệ thống thông tin và xử lý khi thấy có thể xảy ra sự cố.

3.4. Hồ sơ xử lý sự cố

a) Quá trình xử lý sự cố phải được ghi chép và lưu trữ tại UBND.

b) Thu thập, ghi chép, bảo toàn bằng chứng, chứng cứ phục vụ cho việc kiểm tra, xử lý, khắc phục và phòng ngừa sự cố lặp lại trong tương lai. Trong trường hợp sự cố về thông tin có liên quan đến các vi phạm pháp luật, đơn vị có trách nhiệm thu thập và cung cấp chứng cứ cho cơ quan có thẩm quyền đúng theo quy định của pháp luật.

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

- Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác

- Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố

Thời gian khắc phục sự cố ATTT:

TT	Loại sự cố	Thời gian phản hồi	Mục tiêu phản hồi đúng thời hạn	Thời gian xử lý (khôi phục)	Mục tiêu khôi phục	Thời gian cập nhật thông tin xử lý
1	M3-Thông thường	60 phút	95%	03 ngày	98%	4 – 8 giờ/lần

5. Quy trình ứng cứu sự cố an toàn thông tin mạng lớn và nghiêm trọng

- Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác

- Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố

- Thông báo ngay cho Ban chỉ huy ứng cứu sự cố và lãnh đạo đơn vị để huy động nhân sự, phương tiện, và phối hợp các bộ phận liên quan. Liên hệ đơn vị chuyên trách hoặc cơ quan chức năng cấp trên (VD: VNCERT/CC) nếu cần hỗ trợ kỹ thuật hoặc điều phối quốc gia.

- Phân tích nguyên nhân, loại bỏ mã độc và lỗ hổng, khôi phục dữ liệu an toàn và giám sát hệ thống sau khi phục hồi.

Thời gian khắc phục sự cố ATTT:

TT	Loại sự cố	Thời gian phản hồi	Mục tiêu phản hồi đúng thời hạn	Thời gian xử lý (khôi phục)	Mục tiêu khôi phục	Thời gian cập nhật thông tin xử lý
1	M1-Nghiêm trọng	10 phút	99%	02 giờ	95%	30 phút/lần
2	M2-Lớn	30 phút	99%	08 giờ	98%	30 – 60 phút/lần

6. Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin: Phối hợp với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao – Công an tỉnh và bên cung cấp dịch vụ thực hiện ứng cứu và khắc phục 24/7 với các sự cố mất ATTT ANM tại UBND.

5.5. Quản lý an toàn người sử dụng đầu cuối

Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:

Yêu cầu	- Quản lý truy cập, sử dụng tài nguyên nội bộ. - Quản lý truy cập mạng và tài nguyên trên Internet.
Hiện trạng	Đáp ứng. - Tham chiếu Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về quy định về đảm bảo an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi. - Đã quy định tại Điều 16, Quyết định 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm: 1. Quản lý truy cập, sử dụng tài nguyên nội bộ

	a) Người sử dụng khi truy cập, sử dụng tài nguyên phải tuân thủ các quy định của pháp luật về bảo đảm ATTT và các quy định của cơ quan, tổ chức. b) Khi cài đặt, kết nối máy tính, thiết bị đầu cuối phải thực hiện theo hướng dẫn, quy trình dưới sự giám sát của bộ phận chuyên trách về ATTT. c) Máy tính, thiết bị đầu cuối phải được xử lý điểm yếu ATTT, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống. 2. Quản lý truy cập, sử dụng tài nguyên trên Internet a) Người dùng được quản lý và kiểm soát truy cập Internet thông qua firewall. b) Các máy trạm đầu cuối được cài đặt phần mềm chống mã độc, cập nhật bản vá hệ điều hành và ứng dụng thường xuyên trước khi kết nối Internet. c) Việc truy cập các dịch vụ đám mây, email cá nhân hoặc tải phần mềm từ Internet phải tuân thủ chính sách của đơn vị; các hành vi vi phạm sẽ bị ngăn chặn và xử lý. d) Hoạt động truy cập Internet được lưu vết (log) và giám sát nhằm phát hiện sớm nguy cơ tấn công hoặc rò rỉ dữ liệu. đ) Chỉ những người dùng được ủy quyền mới được phép sử dụng các dịch vụ công cộng qua Internet để trao đổi công việc. 3. Chính sách, quy trình quản lý an toàn người sử dụng đầu cuối bao gồm: 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 thiết bị máy tính cá nhân (như máy tính xách tay, thiết bị di động cá nhân, USB, ổ cứng di động...) vào mục đích công việc tại UBND xã Đăk Plô. Hạn chế tối đa việc sử dụng thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu liên quan đến chuyên môn, cán bộ nhân viên và các hoạt động của UBND xã Đăk Plô. 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) Bộ phận 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. đ) 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.

	e) 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.

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

Yêu cầu	Có quy định về quản lý rủi ro an toàn thông tin.
Hiện trạng	Đáp ứng. Tham chiếu Điều 17, Quyết định số 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Quy định về quản lý rủi ro an toàn thông tin: 1. 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	Đáp ứng. Tham chiếu Điều 18, Quyết định 410/QĐ-UBND ngày 27/5/2026 của UBND xã Đăk Plô Về việc ban hành Quy chế bảo đảm an toàn, an ninh mạng Hệ thống thông tin UBND, HĐND xã Đăk Plô.
Phương án	Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau: 1. Thực hiện hủy bỏ toàn bộ thông tin, dữ liệu trên hệ thống với sự xác nhận của đơn vị chủ quản HTTT khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ HTTT. Trong trường hợp thông tin, dữ liệu của HTTT lưu trữ trên tài sản vật lý, đơn vị chủ quản HTTT thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bảo

	đảm không có khả năng phục hồi. Với trường hợp đặc biệt không thể tiêu hủy thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc phần lưu trữ dữ liệu trên tài sản đó. 2. Đối với các HTTT có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ sửa chữa thiết bị lưu trữ dữ liệu

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

Hệ thống thông tin UBND xã Đăk Plô có nhiều hệ thống thành phần khác nhau, trong đó hệ thống thành phần là mạng nội bộ cấp độ 2 (cấp độ cao nhất), được thuyết minh phương án đáp ứng yêu cầu cấp độ 2 như sau:

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

a) 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 biên	Có	Đây là khu vực bố trí các thiết bị quan trọng như Router và Firewall, đóng vai trò trung gian giữa hệ thống mạng nội bộ và Internet. Vùng mạng biên chịu trách nhiệm bảo vệ và quản lý toàn bộ lưu lượng ra vào hệ thống, bao gồm kiểm soát truy cập, lọc gói tin, giám sát an ninh và phát hiện – ngăn chặn các mối đe dọa từ bên ngoài.
2	Vùng mạng nội bộ	Có	Đây là khu vực được thiết kế, bố trí các thiết bị như máy tính, máy in và các thiết bị nội bộ khác, cung cấp dịch vụ cho người dùng. Vùng mạng này cho phép kết nối, chia sẻ dữ liệu và truy cập internet hoặc mạng không dây một cách an toàn, đảm bảo hiệu suất và bảo mật.

3	Vùng mạng khách	Có	Thiết kế, bố trí lắp đặt các thiết bị wifi cung cấp kết nối internet có dây và không dây cho người dân. Vùng mạng này chỉ cho phép truy cập internet, đảm bảo tách biệt với các vùng mạng khác để tăng cường bảo mật.
4	Vùng DMZ	Chưa sử dụng	Được thiết kế để cung cấp các dịch vụ truy cập công cộng từ bên ngoài như: web, email,... hoặc vùng remote mà không làm ảnh hưởng đến hệ thống mạng nội bộ. Khu vực này được đặt giữa lớp tường lửa, nhằm ngăn cách hoàn toàn giữa mạng nội bộ và Internet công cộng.
5	Vùng máy chủ nội bộ	Chưa sử dụng	Được thiết kế sẵn sàng cung cấp dịch vụ với lớp bảo mật cao. Vùng này được cô lập với các vùng mạng khác bằng tường lửa và phân quyền truy cập chặt chẽ nhằm đảm bảo hiệu suất, độ tin cậy và an toàn thông tin cho toàn bộ hệ thống.

b) Phương án thiết kế bảo đảm an toàn thông tin

STT	Yêu cầu	P/A	Ghị chú/Mô tả
1	Có phương án quản lý truy cập, quản trị hệ thống từ phường an toàn sử dụng mạng riêng ảo hoặc phương án tương đương	Đáp ứng	Sử dụng Tường lửa (Firewall) có thích hợp chức năng VPN để quản lý truy cập, quản trị hệ thống từ phường an toàn. Tính năng VPN này được cấu hình trực tiếp trên thiết bị tường lửa (Firewall), quản lý truy cập bên ngoài vào vùng mạng nội bộ. Khi sử dụng VPN, toàn bộ lưu lượng dữ liệu được mã hóa, đi kèm với cơ chế xác thực người dùng, phân quyền và ghi log truy cập, nhờ đó đảm bảo tính bí mật, toàn vẹn và an toàn thông tin trong quá trình quản trị từ xa

2	Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập, sử dụng tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc phương án tương đương	Đáp ứng	Sử dụng Tường lửa có tích hợp chức năng IPS để quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập Tính năng IPS được cấu hình trên Tường lửa kiểm soát truy cập và phòng chống xâm nhập giữa các phân vùng mạng nội bộ.
3	Có phương án phòng chống mã độc cho máy chủ và máy trạm sử dụng sản phẩm phòng chống mã độc hoặc phương án tương đương	Đáp ứng	Sử dụng sản phẩm phòng chống mã độc tập trung của tỉnh triển khai các máy tính trạm, các đơn vị cung cấp dịch vụ là: Bkav…
4	Có phương án phòng chống tấn công mạng cho ứng dụng Web; sử dụng sản phẩm Tường lửa ứng dụng Web đối với hệ thống thông tin quy định tại khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP.	Không	Hệ thống thông tin của đơn vị chưa có máy chủ web. Hiện tại đã thuê đơn vị dịch vụ (đáp ứng hồ sơ cấp độ 3 theo khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP).
5	Có phương án đảm bảo an toàn thông tin cho hệ thống thư điện tử đối với hệ thống thư điện tử	Không	Hệ thống thông tin của đơn vị không có hệ thống thư điện tử. Hiện tại đang sử dụng hệ thống thư điện tử của UBND tỉnh do đơn vị Trung tâm công báo tỉnh Quảng Ngãi vận hành.
6	Phương án dự phòng cho các thiết bị chính	Chưa đáp ứng	Đơn vị sẽ đầu tư các thiết bị dự phòng như: Tường lửa (Firewall), Switch trong vòng 12 tháng kể từ ngày phê duyệt hồ sơ đề xuất cấp độ được phê duyệt.

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.	Đáp ứng	Hệ thống được thiết lập chỉ cho phép kết nối mạng có hỗ trợ mã hóa, xác thực khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet.
2	Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài.	Đáp ứng	Hệ thống thông tin của đơn vị sau khi mua sắm thiết bị tường lửa sẽ cấu hình chặn lọc các dịch vụ không cung cấp, không cho phép
3	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.	Đáp ứng	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng được thiết lập trên Firewall và ngắt phiên kết nối VPN khi người sử dụng không thao tác sử dụng trong 1 khoản thời gian.

1.3 Kiểm soát truy cập từ bên trong mạng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của Đơn vị	Đáp ứng	Chính sách kiểm soát truy cập từ các vùng mạng trong hệ thống đi ra các mạng bên ngoài và mạng Internet được thiết lập trên Tường lửa.

1.4. Nhật ký hệ thống

Yêu cầu thiết bị	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị mạng chính	Sử dụng máy chủ thời gian để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia hoạt động giám sát.
Modem Viettel	+	+
Modem VNPT	+	+
Router/ MikroTik CCR2004-16G-2S+	+	+
Firewall/Sophos XGS 2100 HW	+	+
Ruijie Reyee RG-ES224GC	+	+
Ruijie Reyee RG-ES216GC	+	+
Ruijie Reyee RG-ES208GC	+	+

1.5. Phòng chống xâm nhập

STT	**Yêu cầu**	**P/A**	**Ghi chú/Mô tả**
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống	Đáp ứng	Các vùng mạng được phân tách, triển khai hệ thống IDS/IPS tích hợp trong Tường lửa cho phép phát hiện và phòng chống xâm nhập.

2	Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng (Signatures).	Đáp ứng	Thiết lập chế độ tự động cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng trên hệ thống IDS/IPS tích hợp trong thiết bị tường lửa Firewall.

1.6. Bảo vệ thiết bị hệ thống

Yêu cầu thiết bị	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.	Cấu hình thiết bị (nếu hỗ trợ) chỉ cho phép hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa.
Modem Viettel	+	+	+
Modem VNPT	+	+	+
Router/ MikroTik CCR2004-16G-2S+	+	+	+
Firewall/Sophos XGS 2100 HW	+	+	+
Ruijie Reyee RG-ES224GC	+		
Ruijie Reyee RG-ES216GC	+		
Ruijie Reyee RG-ES208GC	+		

2. Bảo đảm an toàn máy chủ

Hệ thống thông tin UBND, HĐND xã Đăk Plô chưa có nhu cầu sử dụng máy chủ.

3. Bảo đảm an toàn ứng dụng

Hệ thống thông tin UBND, HĐND xã Đăk Plô chưa có nhu cầu sử dụng ứng dụng.

4. Bảo đảm an toàn dữ liệu

4.1. Bảo mật dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ	Đáp ứng	Dữ liệu quan trọng trên hệ thống bao gồm: Dữ liệu nghiệp vụ, văn bản điện tử quan trong và dữ liệu cấu hình hệ thống. Dữ liệu được nén và thiết lập mật khẩu để bảo vệ. tẹo tin lưu trữ phải có mã kiểm tra tính toàn vẹn kèm theo

4.2. 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 cơ bản sau: Tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ	Đáp ứng	Định kỳ hàng tuần sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: Tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ trên thiết bị hoặc hệ thống lưu trữ độc lập.