ỦY BAN NHÂN DÂN TỈNH HƯNG YÊN
ỦY BAN NHÂN DÂN XÃ ĐÌNH DÙ

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ
HỆ THỐNG THÔNG TIN MẠNG LAN
ỦY BAN NHÂN DÂN XÃ ĐÌNH DÙ

ỦY BAN NHÂN DÂN XÃ ĐÌNH DÙ
CHỦ TỊCH

Trần Quang Huy

Văn Lâm - 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 Chủ quản hệ thống thông tin

- Tên tổ chức: UBND tỉnh Hưng Yên.

- Quy định chức năng, nhiệm vụ và quyền hạn: Căn cứ Luật Tổ chức chính quyền địa phương số 77/2015/QH13 ngày 19/6/2015 và Luật sửa đổi, bổ sung một số điều của Luật Tổ chức chính phủ và Luật Tổ chức chính quyền địa phương số 47/2019/QH14 ngày 22/11/2019.

- Người đại diện: Ông Trần Quốc Văn, Chức vụ: Chủ tịch UBND tỉnh.

- Địa chỉ: Số 10, đường Chùa Chuông, thành phố Hưng Yên.

- Thông tin liên hệ: Số điện thoại: 0221.3863823

- Địa chỉ thư điện tử: hungyen@chinhphu.vn

2. Thông tin Đơn vị vận hành

- **Tên Đơn vị vận hành:** UBND Xã Đình Dù.

- Quy định chức năng, nhiệm vụ và quyền hạn: Căn cứ 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 Trần Quang Huy, Chức vụ: Chủ tịch UBND xã.

- Địa chỉ: Xã Đình Dù - Huyện Văn Lâm - Tỉnh Hưng Yên.

- Thông tin liên hệ: 0329.778.809

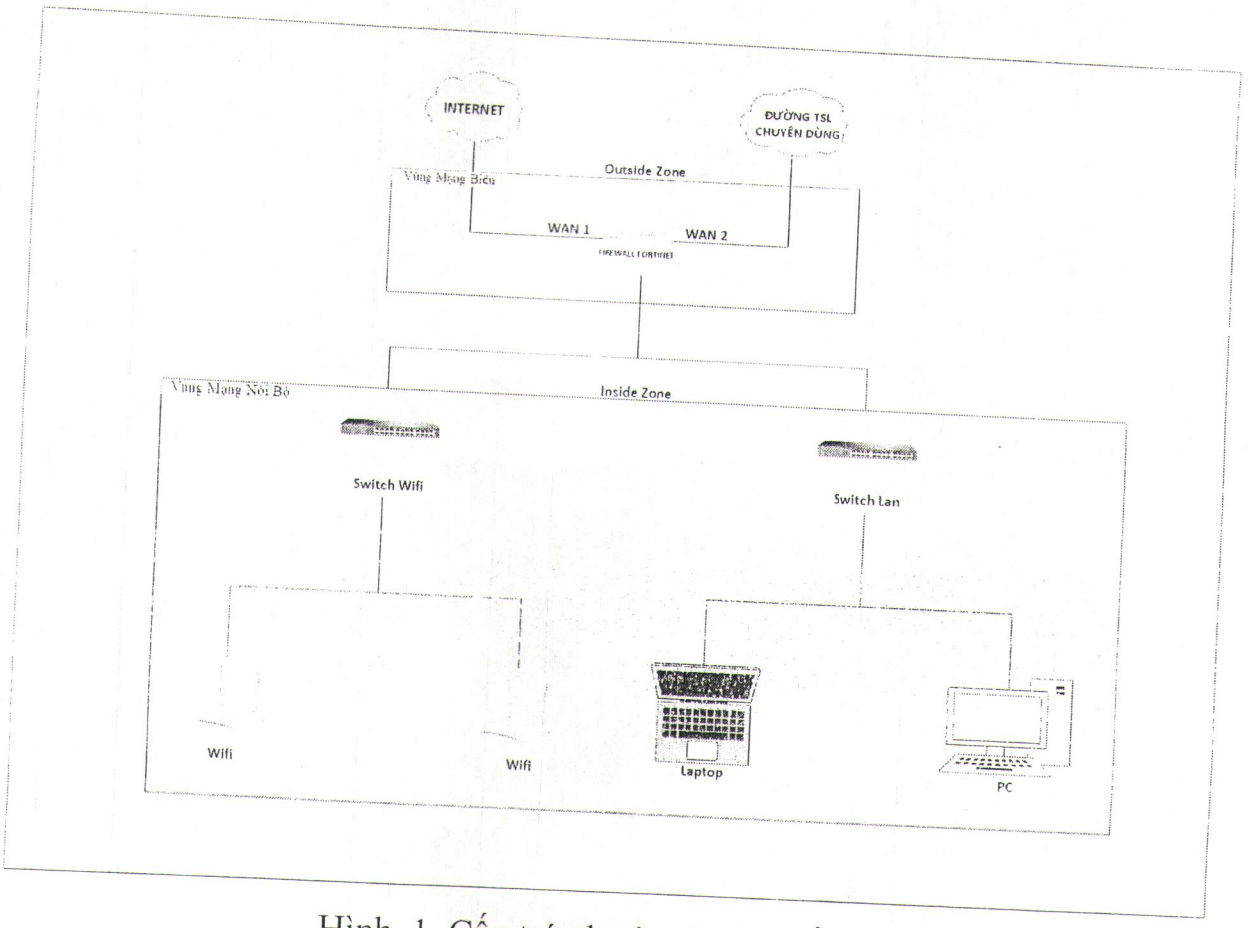
3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của hệ thống mạng LAN: Hệ thống thiết lập để phục vụ công tác chỉ đạo điều hành và cung cấp dịch vụ thông tin trong phạm vi UBND xã Đình Dù.

- Đối tượng phục vụ của hệ thống: Các phòng ban chuyên môn, cán bộ nhân viên làm việc tại Uỷ ban nhân dân xã Đình Dù.

4. Mô tả cấu trúc của hệ thống

4.1. Mô hình logic tổng thể



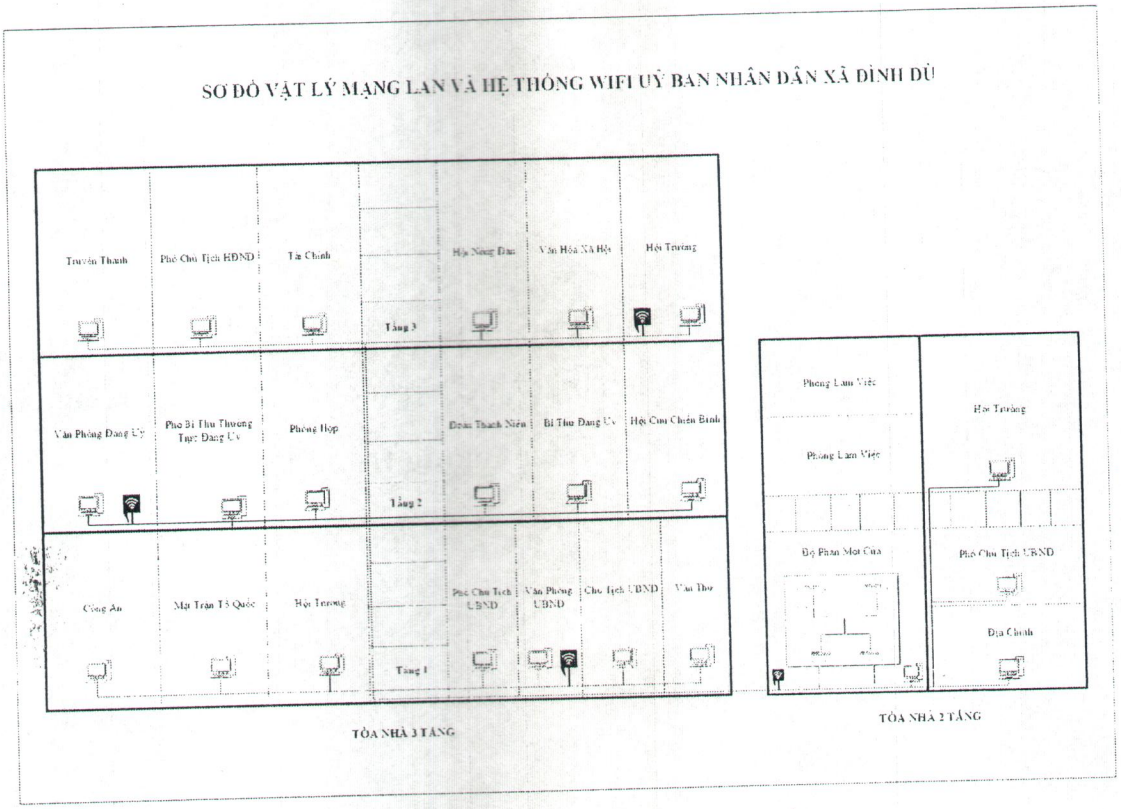
Hình 1. Cấu trúc logic của hệ thống

Mô tả Các vùng mạng được thiết kế như sau:

- Với cấu trúc mạng chính gồm 3 phần mạng Lan, hệ thống mạng nội bộ và mạng Wifi.
- Hệ thống có 1 kênh truyền Internet chạy các ứng dụng kết nối đến Internet khác.
- Hệ thống mạng truyền số liệu chuyên dùng kết nối từ Trung ương tới địa phương, các cơ quan Đảng và Nhà nước, sở ban ngành, các đơn vị từ tỉnh, huyện, xã.
- Hệ thống mạng được quy hoạch theo 3 lớp Core- distribute- access, với các Switch distribute được đặt theo các tầng.
- Hệ thống được trang bị thêm Firewall giúp đảm bảo vấn đề an toàn thông tin trên mạng Internet, cùng với đó là hệ thống Wifi tập trung dễ dàng quản lí và tăng độ phủ sóng, phục vụ tốt cho công việc của cán bộ nhân viên.

4.2. Mô hình kết nối vật lý

Mạng từ nhà cung cấp dịch vụ được kết nối qua thiết bị Fortinet sau đó qua hệ thống switch và chia tới các phòng.



Hình 2. Kết nối vật lý của hệ thống

- Thiết bị tường lửa thực hiện chức năng định tuyến, kiểm soát truy cập, băng thông, và bảo vệ máy tính người dùng trong hệ thống.
- Thiết bị chuyển mạch Switch cho các tầng và phòng ban thực hiện chức năng chuyển mạch cho toàn bộ người dùng trong hệ thống.
- Switch Wifi đảm bảo hoạt động cho hệ thống Wifi, giúp người dùng sử dụng Wifi nhanh và ổn định.
- Các máy tính của cán bộ nhân viên chủ yếu thực hiện các tính năng như gửi, nhận văn bản, tin học văn phòng, các phần mềm nội bộ và in ấn tài liệu.

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	Thiết bị tường lửa Fortiner 60F	Vùng Mạng Biên	Cách ly toàn bộ dữ liệu giữa mạng nội bộ và ngoài Internet.
2	Siwtch Lan Tp-Link	Vùng Mạng Nội Bộ	Thực hiện chức năng chuyển mạch cho toàn bộ người dùng trong hệ thống.

3	Switch Wifi Tp-Link	Vùng Mạng Nội Bộ	Cung cấp mạng cho các thiết bị Wifi được lắp tại đơn vị.
4	Wifi Tp-Link	Vùng Mạng Nội Bộ	Phát Wifi cho các thiết bị của cán bộ nhân viên sử dụng.

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

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

STT	Vùng mạng	IP Private	IP Public
1	Mạng nội bộ	10.112.78.1	117.2.113.119

Bảng 2. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

PHẦN II.

THUYẾT MINH ĐỀ XUẤT CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

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

Hệ thống thông tin thuộc phạm vi quản lý của Uỷ ban nhân dân xã Đình Dù bao gồm các hệ thống thông tin với cấp độ đề xuất tương ứng, cụ thể:

STT	Hệ thống	Loại hình HTTT	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống mạng nội bộ Lan và hệ thống mạng Wifi.	Hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức và chỉ xử lý thông tin công cộng	1	Điều 7 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 (LAN) xử lý thông tin công khai và phục vụ hoạt động nội bộ cho cán bộ của UBND xã Đình Dù. Căn cứ Điều 7 Nghị định số 85/2016/NĐ-CP, hệ thống này được đề xuất cấp độ 1.

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

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 máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

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 01 tháng, kể từ khi HSĐXCĐ 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 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

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

3.2. Kiểm soát truy cập

3.3. Nhật ký hệ thống

4. Bảo đảm an toàn dữ liệu

4.1. 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 06 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống của UBND Xã Đình Dù 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 và Wifi	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	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 máy chủ và ứng dụng: a) Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phướng án giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị. b) Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường (Ví dụ: user không có quyền nhưng cố tình truy xuất đến các file lưu mật khẩu…). 3. 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. 4. 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, PDA) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích kinh doanh của công ty. 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 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 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 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

Phương án	Xây dựng và công bố Quy chế bảo đảm an toàn thông tin: UBND Xã Đình Dù đã xây dựng, ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin 1. Quy chế được Văn phòng UBND Xã Đình Dù xây dựng, lấy ý kiến tất cả công chức, viên chức và người lao động cơ quan. 2. Quy chế được Văn phòng UBND Xã Đình Dù hoàn thiện trình Lãnh đạo xã 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
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 về Sở Thông tin và Truyền thông để tổng hợp báo cáo Uỷ ban nhân dân tỉnh 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
Phương án	UBND Xã Đình Dù ban hành Quyết định giao cán bộ công chức văn phòng xã vận hành về an toàn thông tin.

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	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) UBND Xã Đình Dù giao cán bộ công chức văn phòng xã là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin. b) Cán bộ công chức văn phòng xã 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 xã. c) Cán bộ công chức văn phòng xã chủ trì, phối hợp với Sở Thông tin và Truyền thông, phòng Văn hóa thông tin huyện 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. 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: Tùy theo mức độ sự cố, phối hợp Cục An toàn thông tin hoặc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam 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
Phương án	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.

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
Phương án	Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ:

	a) Quy định 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. b) Có chuyên gia trong lĩnh vực đánh giá, kiểm tra trình độ chuyên môn phù hợp với vị trí tuyển dụng.

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	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. - Cá nhân, tổ chức 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. b) Với 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.
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	Có hình thức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng.

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
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 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	Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.
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 Quy chế bảo đảm an toàn, an ninh mạng hệ thống.
Phương án	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

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	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: 1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống, trình cấp có thẩm quyền phê duyệt, trước khi thực hiện thử nghiệm và nghiệm thu hệ thống. 2. Hệ thống phải được thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng theo nội dung, kế hoạch được phê duyệt.

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	Quy định về quản lý an toàn mạng: 1. Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật. 2. Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên ngoài mạng; Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.

5.1.5.2. 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	Quy định về quản lý an toàn máy chủ và ứng dụng: 1. Quy định với máy chủ a) Hệ thống máy chủ phải có tính năng sẵn sàng cao, cơ chế dự phòng linh hoạt để đảm bảo hoạt động liên tục. b) Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt, động đất và các thảm họa khác do thiên nhiên hoặc con người gây ra và các phương án khôi phục sau thảm họa cho hệ thống máy chủ. c) Máy chủ phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Thực hiện biện pháp phòng chống xâm nhập; Phòng chống phần mềm độc hại và xử lý dữ liệu trên máy chủ khi chuyển giao. d) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. đ) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và thực hiện theo quy trình đã được phê duyệt. e) Phần mềm hệ điều hành cài lên máy chủ ưu tiên là phần mềm hệ điều hành có bản quyền hoặc là phần mềm mã nguồn mở được sử dụng rộng rãi trong nước và quốc tế. g) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. 2. Quy định với ứng dụng: a) Các yêu cầu, thiết kế về an toàn bảo mật của phần mềm ứng dụng cần được xác định rõ trong tài liệu phân tích, thiết kế. Trong quá trình triển khai, vận hành các phần mềm ứng dụng cần đảm bảo nghiêm ngặt theo các yêu cầu, thiết kế về an toàn bảo mật. b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Kết nối về hệ thống giám sát tập trung; Có phương án bảo mật thông tin liên lạc, chống chối bỏ và biện pháp bảo đảm an toàn ứng dụng và mã nguồn. c) Có phương án xác định và khắc phục rủi ro trước, trong quá trình triển khai và khi vận hành các phần mềm ứng dụng.

	d) Ứng dụng phải kiểm tra, thử nghiệm và có biên bản đánh giá tính an toàn, bảo mật đối với phần mềm ứng dụng theo yêu cầu khi nghiệm thu các phần mềm này. Việc tiến hành thử nghiệm phải đảm bảo trên môi trường riêng biệt, không ảnh hưởng tới hoạt động và dữ liệu của đơn vị.

5.1.5.3. 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	Quy định về quản lý an toàn dữ liệu: 1. Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn. 2. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. 3. Tiến hành cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ được thực hiện theo yêu cầu của đơn vị vận hành hệ thống. 4. Sử dụng mật mã để bảo đảm an toàn và bảo mật dữ liệu trong lưu trữ. 5. Quản lý chặt chẽ các thiết bị lưu trữ dữ liệu, nghiêm cấm việc di chuyển, thay đổi vị trí khi chưa được phép của người có thẩm quyền. 6. Quản lý và phân quyền truy cập phần mềm ứng dụng và cơ sở dữ liệu phù hợp với chức năng, nhiệm vụ của người sử dụng. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên.

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	Phương án quản lý rủi ro an toàn thông tin phải được xây dựng trong Quy chế bảo đảm an toàn, trong đó cần làm rõ các nội dung sau đây: 1. Xác định mức rủi ro. 2. Quy trình đánh giá và quản lý rủi ro. 3. Biện pháp kiểm soát rủi ro.

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	Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ phải được xây dựng trong Quy chế bảo đảm an toàn, trong đó cần làm rõ các nội dung sau đây: 1. Quy định về bảo đảm an toàn thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ. 2. Quy trình xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ. 3. Phương án kỹ thuật thực hiện xử lý thông tin trên hệ thống khi thay đổi mục đích sử dụng hoặc gỡ bỏ.

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, công chức, viên chức, nhân viên của UBND Xã Đình Dù. 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 hệ thống ra bên ngoài Internet và các mạng khác.

b) Phương án thiết kế bảo đảm các yêu cầu:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập	Có	Các thiết bị hệ thống Sử dụng tường lửa Firewall Fortinet quản lý truy cập từ bên ngoài vào vùng mạng nội bộ.
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Có	Truy cập giữa các vùng mạng được quản lý và phòng chống xâm nhập sử dụng Modem có tích hợp chức năng phòng chống xâm nhập IPS.
3	Phương án phòng chống mã độc cho	Có	Sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương (Giải pháp cài đặt phần mềm virus BKAV Endpoint).

	máy chủ và máy trạm		

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	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 thông qua Modem.

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	+
Firewall/Fortigate	+
Switch L2/Tp-Link	+
Switch/Wifi/Tp-Link	+

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	Có	Các vùng mạng được triển khai hệ thống IPS, hoạt động ở chế độ Inline 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	Có	Đã thiết lập chức năng tự động cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng đều được thiết lập trên các thiết bị IPS.

5.2.1.5. 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.
Modem	+	+
Firewall/Fortigate	+	+
Switch L2/Tp-link	+	+
Switch/Wifi/Tp-Link	+	+

5.2.2. Bảo đảm an toàn ứng dụng

5.2.2.1. Xác thực

Yêu cầu / **Ứng dụng**	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
Mạng Nội bộ (LAN)	+	+	+

5.2.2.2. Kiểm soát truy cập

Yêu cầu / **Ứng dụng**	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
Mạng Nội bộ (LAN)	+	+

5.2.2.3. Nhật ký hệ thống

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

5.2.3. Bảo đảm an toàn dữ liệu

5.2.3.1. Sao lưu dự phòng.

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu quan trọng trên hệ thống	Có	Thông tin, dữ liệu quan trọng trên hệ thống đảm bảo được sao lưu dự phòng như: tập tin cấu hình hệ thống, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.