

ỦY BAN NHÂN DÂN TỈNH ĐẮK NÔNG
HUYỆN ĐẮK GLONG

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ
HỆ THỐNG THÔNG TIN HUYỆN ĐẮK GLONG

Đắk Glong – 2024

MỤC LỤC

MỤC LỤC	1
THUẬT NGỮ, TỪ VIẾT TẮT.....	1
DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ	3
PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN.....	4
1. Thông tin Chủ quản hệ thống thông tin.....	4
2. Thông tin Đơn vị vận hành.....	4
3. Mô tả phạm vi, quy mô của hệ thống	4
4. Mô tả cấu trúc của hệ thống.....	5
PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT	11
1. Danh mục hệ thống thông tin và cấp độ đề xuất.....	11
2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin.....	11
PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN	12
PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 2	14
6.1.1. Thiết lập chính sách an toàn thông tin.....	14
6.1.2. Tổ chức bảo đảm an toàn thông tin.....	19
6.1.3. Bảo đảm nguồn nhân lực.....	21
6.1.4. Quản lý thiết kế, xây dựng hệ thống thông tin	23
6.1.5. Quản lý vận hành hệ thống thông tin.....	28
PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÀNH PHẦN CẤP ĐỘ 2	36
6.2.1. Bảo đảm an toàn mạng	36

6.2.2. Bảo đảm an toàn máy chủ	39
6.2.3. Bảo đảm an toàn ứng dụng	43
6.2.4. Bảo đảm an toàn dữ liệu.....	44

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	HSDXCD	Hồ sơ đề xuất cấp độ
4	LAN	Mạng nội bộ
5	WAN	Mạng tin học diện rộng
6	VNP	Vitural Private Network
7	DNS	Domain Name Server

DANH MỤC CÁC BẢNG

Bảng 1. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống	10
Bảng 2. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống.....	10

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

Hình 1. Cấu trúc logic của hệ thống.....	5
Hình 2. Kết nối vật lý của hệ thống	7

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

1. Thông tin Chủ quản hệ thống thông tin

- **Tên Tổ chức: UBND huyện Đắk Glong.**

- Được thành lập theo Nghị định 82/2005/NĐ-CP ngày 27/6/2005 của Thủ tướng Chính phủ về việc thành lập thị xã Gia Nghĩa, thành lập các phường, xã thuộc thị xã Gia Nghĩa và đổi tên huyện Đắk Nông thành huyện Đắk Glong, tỉnh Đắk Nông.

- Người đại diện: Ông Trần Nam Thuận, Phó Bí thư - Chủ tịch UBND huyện.

- Địa chỉ: xã Quảng Khê, huyện Đắk Glong, tỉnh Đắk Nông.

- Thông tin liên hệ: 0913464768; - Email: dakglong@daknong.gov.vn.

2. Thông tin Đơn vị vận hành

2.1. Đơn vị vận hành mạng Lan UBND huyện

- Tên Đơn vị vận hành: Phòng Văn hóa và Thông tin huyện Đắk Glong.

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 03/QĐ-UBND ngày 28/11/2023 của UBND huyện Đắk Glong Quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Phòng Văn hóa và Thông tin huyện Đắk Glong.

- Người đại diện: Ông Nguyễn Hồng Thanh, Chức vụ: Trưởng phòng

- Địa chỉ: xã Quảng Khê, huyện Đắk Glong, tỉnh Đắk Nông

- Thông tin liên hệ 0394523968;

- Email: thanhnh.pvhtt.dakglong@daknong.gov.vn.

2.2. Đơn vị vận hành Trang thông tin điện tử huyện Đắk Glong

- Tên tổ chức: Trung tâm Dữ liệu Công nghệ và Truyền thông tỉnh Đắk Nông

- Người đại diện: Ông Ngô Văn Đức - Giám đốc Trung tâm.

- Địa chỉ: Tầng 3 trụ sở Sở Thông tin và Truyền thông tỉnh Đắk Nông, đường 23/3, phường Nghĩa Đức, thành phố Gia Nghĩa, tỉnh Đắk Nông.

- Thông tin liên hệ: 02613.701.166 Email: dlcntt.stttt@daknong.gov.vn

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống thông tin: Hệ thống thông tin UBND huyện Đắk Glong được thiết lập để phục vụ công tác ứng dụng công nghệ thông tin, chuyển đổi số của UBND huyện Đắk Glong.

- Đối tượng phục vụ của hệ thống: Công chức, viên chức, người lao động và cơ quan, tổ chức khác liên quan đến việc cung cấp ứng dụng CNTT, chuyển đổi số của UBND huyện Đắk Glong.

- Danh mục các hệ thống thông tin thành phần:

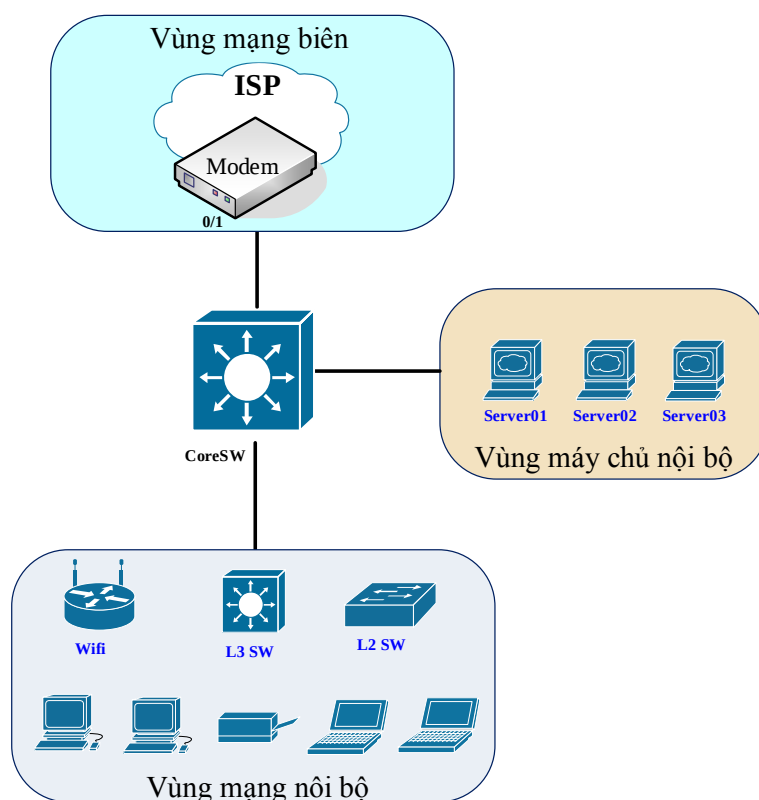
+ Hệ thống mạng nội bộ (LAN) trụ sở UBND huyện Đắk Glong;

+ Trang thông tin điện tử huyện Đắk Glong.

4. Mô tả cấu trúc của hệ thống

4.1. Mô hình logic tổng thể

a) Sơ đồ của hệ thống



Hình 1. Cấu trúc logic của hệ thống hiện tại

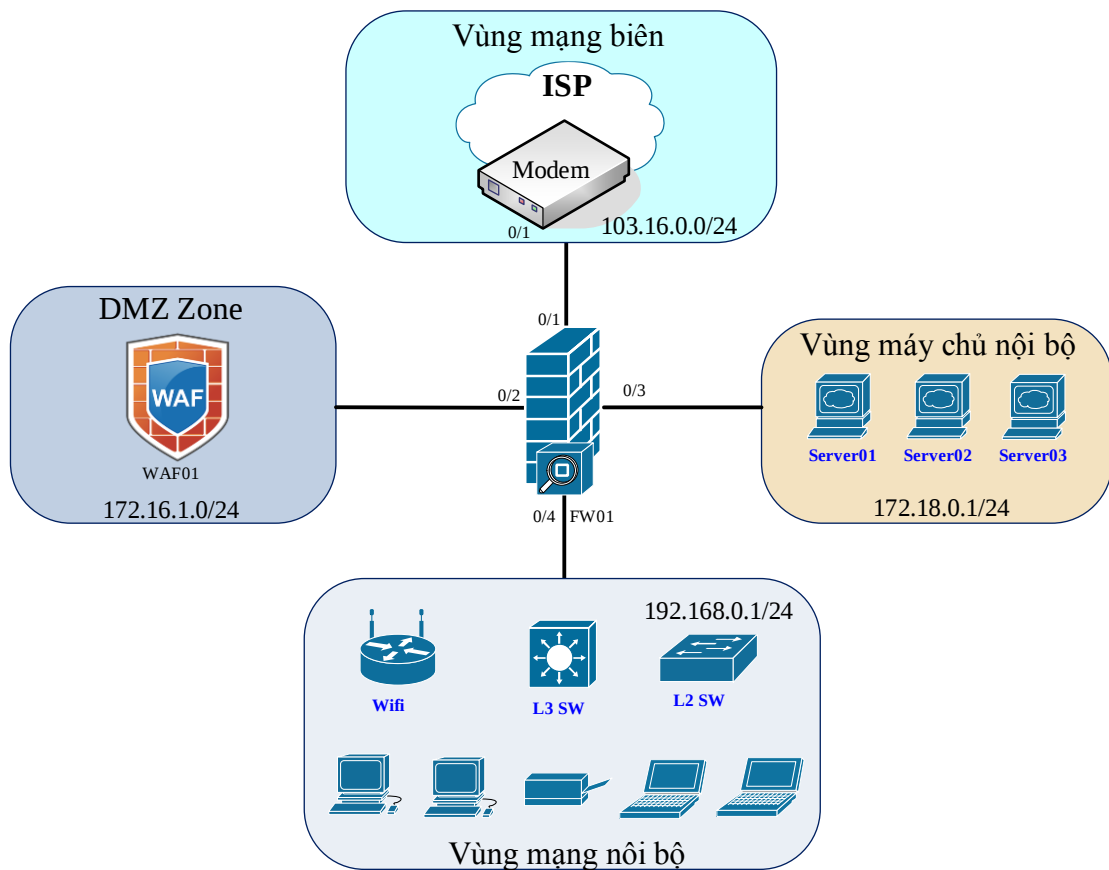
Các vùng mạng được thiết kế như sau:

+ Vùng mạng biên được thiết kế để kết nối hệ thống mạng LAN trụ sở UBND huyện Đắk Glong ra các mạng bên ngoài và mạng Internet; bảo vệ hệ thống từ bên ngoài Internet; Vùng mạng này triển khai thiết bị cung cấp cổng kết nối VPN;

+ Vùng máy chủ nội bộ đặt máy chủ nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống;

+ Vùng mạng nội bộ đặt các máy tính của người sử dụng;

b) Sơ đồ hệ thống quy hoạch mới để đáp ứng các yêu cầu an toàn



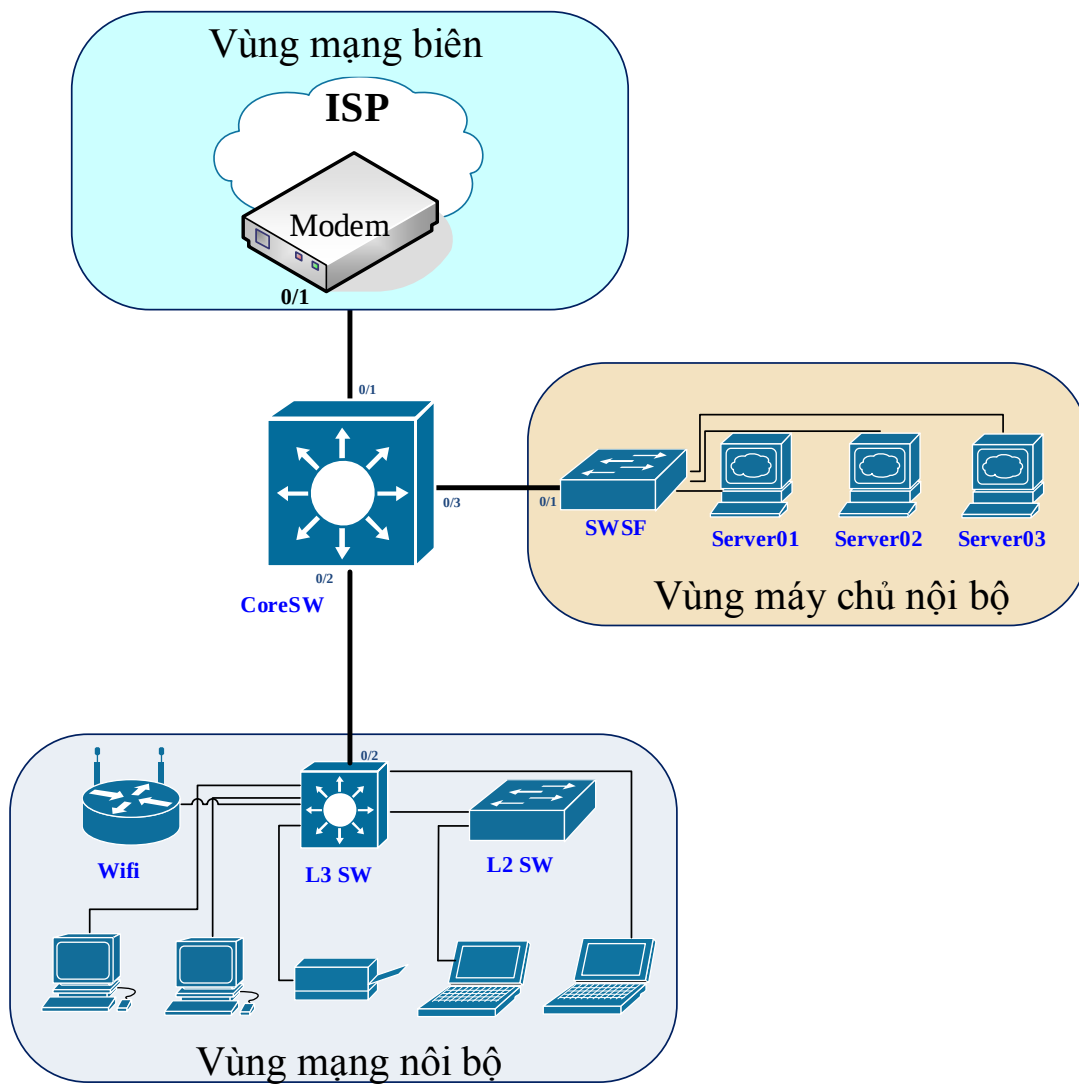
Hình 2. Cấu trúc logic của hệ thống theo quy hoạch mới

Các vùng mạng được thiết kế như sau:

- Vùng mạng biên được đặt các thiết bị Router, Firewall để kết nối hệ thống ra các mạng bên ngoài và mạng Internet.
- Vùng DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet.
- Vùng máy chủ nội bộ (Server Farm) đặt các máy chủ nội bộ, máy chủ cơ sở dữ liệu, cung cấp các dịch vụ/chuyên ngành cho người sử dụng trong hệ thống.
- Vùng mạng nội bộ: đặt các máy tính của người sử dụng.

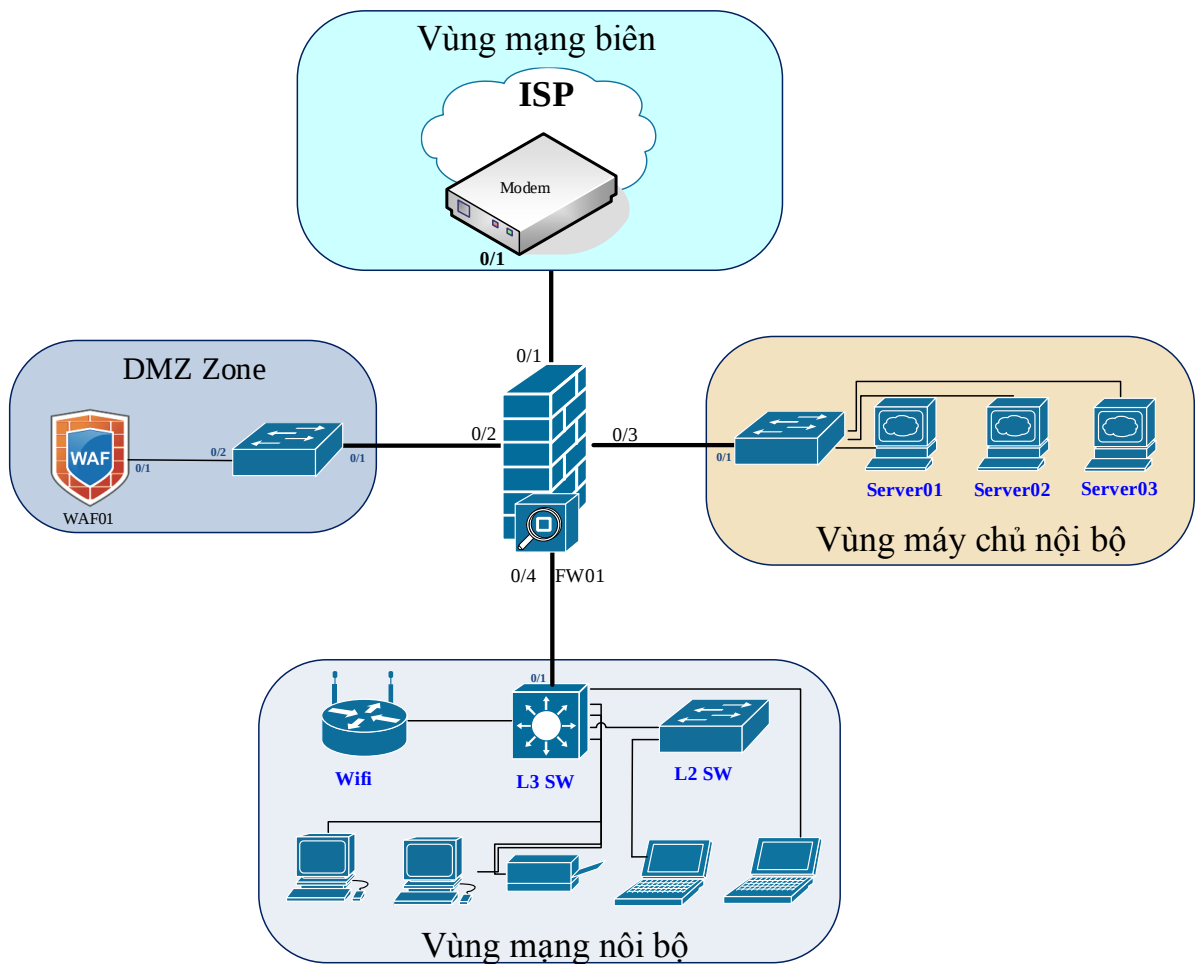
4.2. Mô hình kết nối vật lý

a) Sơ đồ kết nối vật lý



Hình 3. Kết nối vật lý của hệ thống

b) Sơ đồ kết nối vật lý theo quy hoạch mới



4.3. Danh mục thiết bị sử dụng trong hệ thống

a) Danh mục thiết bị đang sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Modem/VNPT	Vùng mạng biên	Kết nối và định tuyến động với các Router của ISP.
2	CoreSW/Cisco3750	Vùng mạng DMZ	Kết nối các vùng mạng của hệ thống
3	SWSF/ Cisco2960	Vùng máy chủ nội bộ	Thiết bị định tuyến quản lý, kết nối vùng máy chủ nội bộ
4	L2 SW/ Cisco2960	Vùng mạng nội bộ	Kết nối các máy trạm và thiết bị đầu cuối trong vùng mạng LAN.

5	L3 SW/ Cisco2960	Vùng mạng nội bộ	Kết nối, định tuyến các Vlan trong mạng nội bộ.
---	------------------	------------------	---

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

b) Danh mục thiết bị bổ sung theo quy hoạch mới

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	FW01/Fortinet200D	Vùng mạng biên	Quản lý truy cập vào/ra và bảo vệ vùng DMZ; Vùng máy chủ nội bộ; Vùng mạng biên.
2	WAF01/V2-WAF	Vùng mạng DMZ	Thiết bị tường lửa bảo vệ ứng dụng web.

Bảng 2. Danh mục thiết bị bổ sung theo quy hoạch mới

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Server 01/Dell PowerEdge R250	Vùng máy chủ nội bộ	Máy chủ cài đặt ứng dụng Web
2	Server 02/Dell PowerEdge R250	Vùng máy chủ nội bộ	Lưu trữ CSDL của hệ thống
3	Server 03/Dell PowerEdge R250	Vùng máy chủ nội bộ	Máy chủ cài đặt app hệ thống

Bảng 3. Danh mục thiết bị máy chủ 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/HDH	Mục đích sử dụng
1	Trang thông tin điện tử	Cấu hình máy chủ IBM Server, Dung lượng 120GB, CPU 4 Core, Ram 8GB	

		Công nghệ website: Nukeviet 3.0 Database: MariaDB Tên miền: dakglong.daknong.gov.vn (IP:103.147.100.138) Đặt tại Trung tâm Dữ liệu Công nghệ và Truyền thông tỉnh Đắk Nông	Truyền tải thông tin các hoạt động của UBND huyện
--	--	--	---

Bảng 1. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

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

STT	Vùng mạng	IP Private	IP Public
1	Vùng máy DMZ	172.16.1.0/24	
2	Vùng máy chủ nội bộ	172.18.0.1/24	
3	Vùng mạng biên	103.147.0.0/24	103.147.0.0/24
4	Vùng mạng LAN	192.168.0.1/24	

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

PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

Hệ thống thông tin thuộc phạm vi quản lý của UBND huyện Đắk Glong bao gồm các hệ thống thông tin với cấp độ đề xuất tương ứng, bao gồm:

STT	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống Mạng nội bộ	2	Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP
2	Trang thông tin điện tử UBND huyện Đắk Glong	1	Điều 7 Nghị định 85/2016/NĐ-CP

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

- Hệ thống mạng LAN UBND huyện Đắk Glong được xây dựng để phục vụ hoạt động nội bộ của cơ quan, tổ chức 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 theo quy định của pháp luật, căn cứ theo quy định tại Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP, hệ thống này được đề xuất cấp độ 2.

- Hệ thống Trang thông tin điện tử UBND huyện Đắk Glong là hệ thống thông tin phục vụ hoạt động nội bộ của cơ quan, tổ chức và chỉ xử lý thông tin công cộng, căn cứ theo quy định tại Điều 7 Nghị định 85/2016/NĐ-CP, hệ thống này được đề xuất cấp độ 1.

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

I. 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.

- Quản lý sự cố an toàn thông tin.

- Quản lý an toàn người sử dụng đầu cuối.

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.

II. 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 12 tháng**, kể từ khi HSDXCD được phê duyệt.

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống thông tin UBND huyện Đắk Glong 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 kỹ thuật đối với Hệ thống Mạng LAN	2	Phụ lục I
2	Thuyết minh phương án đáp ứng yêu cầu kỹ thuật đối với Hệ thống Trang thông tin điện tử	1	Phụ lục II

PHỤ LỤC I

THUYẾT MINH PHƯƠNG ÁN ĐÁP ỨNG YÊU CẦU KỸ THUẬT ĐỐI VỚI HỆ THỐNG MẠNG LAN VỚI CẤP ĐỘ 2

Hệ thống mạng LAN UBND huyện Đắk Glong được xây dựng để phục vụ hoạt động nội bộ của cơ quan, tổ chức 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 theo quy định của pháp luật, căn cứ theo quy định tại Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP, hệ thống này được đề xuất cấp độ 2.

6.1.1. Thiết lập chính sách an toàn thông tin

6.1.1.1. 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 (Tham chiếu Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Quản lý an toàn mạng (Tham chiếu Điều 10 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024) 1. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống. 2. 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. 3. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc. 4. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống. 5. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: a) 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, DVD hoặc SAN.

	b) 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. 6. Truy cập và quản lý cấu hình hệ thống: a) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TLS, SSH, VPN. b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN. c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập. Quản lý an toàn máy chủ và ứng dụng <i>(Tham chiếu Điều 11 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)</i> Quy định về quản lý an toàn máy chủ và ứng dụng: 1. Quy định với máy chủ a) Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng. b) Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ 01 tháng/lần. c) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. d) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và xóa sạch dữ liệu. đ) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. 2. Quy định với ứng dụng: a) Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng. b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Có phương án bảo mật thông tin liên lạc và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.
--	---

	c) Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin 2 năm/lần hoặc khi thay đổi, nâng cấp mở rộng. 3. Truy cập mạng của máy chủ: a) Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống. b) Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có). c) Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN. 4. Truy cập và quản trị máy chủ và ứng dụng: a) Định kỳ 03 tháng thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng. b) Chỉ cấp quyền quản lý máy chủ và ứng dụng cho cán bộ quản trị theo chức năng nhiệm vụ được giao. c) Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN. d) Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN. 5. Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: a) Định kỳ hàng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập. b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn. c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập. Quản lý an toàn dữ liệu <i>(Tham chiếu Điều 12 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)</i> 1. Quy định dự phòng và khôi phục dữ liệu:
--	--

	a) Định kỳ hàng tuần phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập. b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn. c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập. 2. Định kỳ hàng tháng 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. 3. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập. Quản lý sự cố an toàn thông tin <i>(Tham chiếu Điều 13 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)</i> 1. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác. 2. 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. 3. Liên hệ với đầu mối ứng cứu sự cố theo thông tin đưa ra dưới đây: a) Sở Thông tin và Truyền thông tỉnh Đắk Nông - Người liên hệ: Trần Minh Lâm - Số điện thoại: 0848300009. - Email: lamtm.sttt@daknong.gov.vn. b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC). - Người liên hệ/bộ phận: Phòng Ứng cứu sự cố - Số điện thoại: 0869 100 317 - Email: ir@vncert.vn - Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn
--	--

	- Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn. Quản lý an toàn người sử dụng đầu cuối <i>(Tham chiếu Điều 14 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)</i> 1. Khi kết nối thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu. 2. 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 mạng quản trị hoặc nghiệp vụ. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu. 3. Thiết lập mạng công cộng cho 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 và có quản lý truy cập vùng mạng này với các vùng mạng khác trong hệ thống. 4. Máy tính người sử dụng phải được thiết lập chế độ cập nhật bản vá tự động và phần mềm phòng chống mã độc.
--	---

6.1.1.2. 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 <i>(Tham chiếu Điều 20 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)</i>
Phương án	Quy chế này được tổ chức/bộ phận trình người đứng đầu đơn vị vận hành trước khi công bố áp dụng.

6.1.1.3. 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 <i>(Tham chiếu Điều 21 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)</i>

Phương án	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.
------------------	---

6.1.2. Tổ chức bảo đảm an toàn thông tin

6.1.2.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Có công chức có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin.
Hiện trạng	Đáp ứng (Tham chiếu Điều 6 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	1. Giao Phòng Văn hóa và Thông tin là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin 2. Tuân thủ các quy định về trách nhiệm của bộ phận chuyên trách về an toàn thông tin được giao tại Quy chế này.

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

6.1.2.2.a. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin

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
Hiện trạng	Đáp ứng (Tham chiếu Điều 5 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Giao Phòng Văn hóa và Thông tin huyện Đắk Glong là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin.

6.1.2.2.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

Yêu cầu	Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin
Hiện trạng	Đáp ứng (Tham chiếu Điều 5 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: 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) Sở Thông tin và Truyền thông tỉnh Đắk Nông - Người liên hệ: Trần Minh Lâm. - Số điện thoại: 0848300009 - Email: lamtm.sttt@daknong.gov.vn b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC) - Người liên hệ/bộ phận: Phòng Ứng cứu sự cố. - Số điện thoại: 0869 100 317. - Email: ir@vncert.vn. - Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn - Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn

6.1.2.2.c. Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền

Yêu cầu	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 Điều 6 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)

Phương án	Bộ phận chuyên trách về an toàn thông tin là đầu mối tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền
------------------	--

6.1.3. Bảo đảm nguồn nhân lực

6.1.3.1. Tuyển dụng

Yêu cầu	Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng.
Hiện trạng	Đáp ứng
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: 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 phù hợp với vị trí tuyển dụng.

6.1.3.2. Trong quá trình làm việc

6.1.3.2.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

Yêu cầu	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 (<i>Tham chiếu Điều 6 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024</i>)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: 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. - Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT. - 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 quản lý và vận hành hệ thống phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin. - Cán bộ quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin.
--	--

6.1.3.2.b. 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

Yêu cầu	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 Điều 6 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Kế hoạch và định kỳ hàng năm tổ chức đào tạo về an toàn thông tin cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống.

6.1.3.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu 6.1.3.3.a	Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức
--	---

Hiện trạng	Đáp ứng (Tham chiếu Điều 6 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: 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) Bộ phận chuyên trách vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

Yêu cầu 6.1.3.3.b	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 Điều 6 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách về an toàn thông tin 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.

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

6.1.4.1. Thiết kế an toàn hệ thống thông tin

6.1.4.1.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

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
Hiện trạng	Đáp ứng (Tham chiếu Điều 7 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)

Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.
------------------	--

6.1.4.1.b. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin

Yêu cầu	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin
Hiện trạng	Đáp ứng (Tham chiếu Điều 7 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

6.1.4.1.c. Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ

Yêu cầu	Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ
Hiện trạng	Đáp ứng (Tham chiếu Điều 7 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách xây dựng tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

6.1.4.1.d. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin

Yêu cầu	Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin
Hiện trạng	Đáp ứng (Tham chiếu Điều 7 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống.

6.1.4.1.d. 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

Yêu cầu	Có quy định 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 Điều 7 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách 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, báo cáo Lãnh đạo quyết định trước khi thực hiện thay đổi.

6.1.4.2. Phát triển phần mềm thuê khoán

6.1.4.2.a. 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	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
----------------	--

Hiện trạng	Đáp ứng (Tham chiếu Điều 8 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Quy định đối với việc 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.

6.1.4.2.b. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm

Yêu cầu	Có quy định yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm
Hiện trạng	Đáp ứng (Tham chiếu Điều 8 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Quy định đối với việc phát triển phần mềm thuê khoán: a) Các nhà phát triển cung cấp mã nguồn phần mềm cho bộ phận chuyên trách. b) Bộ phận chuyên trách có trách nhiệm quản lý và lưu trữ mã nguồn an toàn.

6.1.4.3. Thử nghiệm và nghiệm thu hệ thống

6.1.4.3.a. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng

Yêu cầu	Có quy định về việc thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng
Hiện trạng	Đáp ứng (Tham chiếu Điều 9 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)

Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: 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 trước khi thực hiện thử nghiệm và nghiệm thu hệ thống. 2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ.
------------------	---

6.1.4.3.b. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có yêu cầu về nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng (Tham chiếu Điều 9 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: Bộ phận chuyên trách và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, trình Lãnh đạo đơn vị phê duyệt trước khi đưa hệ thống vào vận hành, khai thác.

6.1.4.3.c. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống
Hiện trạng	Đáp ứng (Tham chiếu Điều 9 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: Bộ phận chuyên trách phối hợp với bên triển khai hệ thống thực hiện thử nghiệm và nghiệm thu hệ thống, trước khi đưa vào vận hành, khai thác.

6.1.5. Quản lý vận hành hệ thống thông tin

6.1.5.1. Quản lý an toàn mạng

6.1.5.1.a. Quản lý, vận hành hoạt động bình thường của hệ thống

Yêu cầu	Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống
Hiện trạng	Đáp ứng (Tham chiếu Điều 10 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Quy định về quản lý an toàn mạng: 1. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống. 2. 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. 3. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc. 4. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống.

6.1.5.1.b. Cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố

Yêu cầu	Có quy định về cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố
Hiện trạng	Đáp ứng (Tham chiếu Điều 10 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	5. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: a) 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, DVD hoặc SAN.

	b) 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.
--	---

6.1.5.1.c. Truy cập và quản lý cấu hình hệ thống

Yêu cầu	Truy cập và quản lý cấu hình hệ thống
Hiện trạng	Đáp ứng (Tham chiếu Điều 10 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	6. Truy cập và quản lý cấu hình hệ thống: a) Cấu hình hệ thống từ xa phải sử dụng các giao thức bảo mật có mã hóa thông tin như SSL, TLS, SSH, VPN. b) Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN. c) Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập.

6.1.5.2. Quản lý an toàn máy chủ và ứng dụng

6.1.5.2.a. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ

Yêu cầu	Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ
Hiện trạng	Đáp ứng (Tham chiếu Điều 11 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Quy định về quản lý an toàn máy chủ và ứng dụng: 1. Quy định với máy chủ a) Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng. b) Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ 01 tháng/lần.

	c) Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. d) Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và xóa sạch dữ liệu. đ) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ. 2. Quy định với ứng dụng: a) Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng. b) Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Có phương án bảo mật thông tin liên lạc và biện pháp bảo đảm an toàn ứng dụng và mã nguồn. c) Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin 2 năm/lần hoặc khi thay đổi, nâng cấp mở rộng.
--	---

6.1.5.2.b. Truy cập mạng của máy chủ

Yêu cầu	Có quy định quản lý truy cập mạng của máy chủ
Hiện trạng	Đáp ứng (Tham chiếu Điều 11 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	3. Truy cập mạng của máy chủ: a) Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống. b) Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có). c) Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN.

6.1.5.2.c. Truy cập và quản trị máy chủ và ứng dụng

Yêu cầu	Có quy định quản lý truy cập và quản trị máy chủ và ứng dụng
Hiện trạng	Đáp ứng (Tham chiếu Điều 11 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)

Phương án	4. Truy cập và quản trị máy chủ và ứng dụng: a) Định kỳ 03 tháng thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng. b) Chỉ cấp quyền quản lý máy chủ và ứng dụng cho cán bộ quản trị theo chức năng nhiệm vụ được giao. c) Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN. d) Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN.
------------------	---

6.1.5.2.d. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố

Yêu cầu	Có quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố
Hiện trạng	Đáp ứng (Tham chiếu Điều 11 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đăk Glông theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	5. Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: a) Định kỳ hàng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập. b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn. c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.

6.1.5.3. Quản lý an toàn dữ liệu

6.1.5.3.a. Chính sách, quy trình dự phòng và khôi phục dữ liệu

Yêu cầu	Có chính sách, quy trình dự phòng và khôi phục dữ liệu
Hiện trạng	Đáp ứng (Tham chiếu Điều 12 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đăk Glông theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)

Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: 1. Quy định dự phòng và khôi phục dữ liệu: a) Định kỳ hàng tuần phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập. b) Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn. c) Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.
------------------	---

6.1.5.3.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

Yêu cầu	Có quy định 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 (<i>Tham chiếu Điều 12 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024</i>)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: 2. Định kỳ hàng tháng 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. 3. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.

6.1.5.4. Quản lý sự cố an toàn thông tin

Yêu cầu	Phương án quản lý sự cố an toàn thông tin mạng
----------------	--

Hiện trạng	Đáp ứng (Tham chiếu Điều 13 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: 1. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác. 2. 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. 3. Liên hệ với đầu mối ứng cứu sự cố theo thông tin đưa ra dưới đây: a) Sở Thông tin và Truyền thông tỉnh Quảng Ninh - Người liên hệ: Trần Minh Lâm - Số điện thoại: 0848300009. - Email: lamtm.stttt@daknong.gov.vn. b) Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC). - Người liên hệ/bộ phận: Phòng Ứng cứu sự cố - Số điện thoại: 0869 100 317 - Email: ir@vncert.vn - Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn - Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn.

6.1.5.5. Quản lý an toàn người sử dụng đầu cuối

Yêu cầu	Có quy định về quản lý truy cập, sử dụng tài nguyên nội bộ
Hiện trạng	Đáp ứng (Tham chiếu Điều 14 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:

	Quản lý an toàn người sử dụng đầu cuối: 1. Khi kết nối thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu. 2. 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 mạng quản trị hoặc nghiệp vụ. 3. Thiết lập mạng công cộng cho 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 và có quản lý truy cập vùng mạng này với các vùng mạng khác trong hệ thống. 4. Máy tính người sử dụng phải được thiết lập chế độ cập nhật bản vá tự động và phần mềm phòng chống mã độc.
--	---

6.1.5.6. 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 (<i>Tham chiếu Điều 15 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024</i>)
Phương án	Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Quy định về Quản lý rủi ro an toàn thông tin: Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau: a. 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.

6.1.5.7. 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 (<i>Tham chiếu Điều 16 Quy chế bảo đảm an toàn, an ninh Hệ thống thông tin của UBND huyện Đắk Glong theo Quyết định số 1406/QĐ-UBND ngày 31/5/2024</i>)
Phương án	Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau: 1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành. 2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xóa bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi. 3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng.

PHỤ LỤC II

THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG TRANG THÔNG TIN ĐIỆN TỬ CẤP ĐỘ 1

- Hệ thống Trang thông tin điện tử của UBND huyện Đắk Glong đặt tại Trung tâm Dữ liệu Công nghệ và Truyền thông tỉnh Đắk Nông, Hệ thống đáp ứng Online 24/7; Hệ thống được sao lưu dữ liệu tự động, có hệ thống bảo mật và phòng chống cháy nổ cơ bản đáp ứng theo Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013 của Bộ Thông tin và Truyền thông quy định áp dụng tiêu chuẩn, quy chuẩn kỹ thuật đối với Trung tâm dữ liệu.

- Phục vụ cho công chức, viên chức, người lao động UBND huyện Đắk Glong; cung cấp các thông tin cần thiết cho các tổ chức, cá nhân.

- Căn cứ theo quy định tại Điều 7 Nghị định số 85/2016/NĐ-CP, 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:

6.2.1. Bảo đảm an toàn mạng

6.2.1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống:

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 bảo đảm an toàn thông tin

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có	Các thiết bị hệ thống/máy chủ được thiết lập cấu hình cho phép quản trị từ xa an toàn.

			Sử dụng thiết bị cân bằng tải chiều ra, tích hợp tường lửa bảo mật được thiết lập để quản lý, kiểm soát truy cập vào/ra giữa hệ thống với vùng mạng nội bộ, vùng mạng biê.
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/VNPT có tích hợp chức năng phòng chống xâm nhập IPS.
3	Phương án phòng chống mã độc cho máy chủ và máy trạm	Có	Sử dụng phần mềm Phòng chống mã độc tập trung của tỉnh; phần mềm diệt virus có bản quyền...

6.2.1.2. 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/VNPT.

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	Có	Hệ thống được thiết lập chỉ cho phép kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể thông qua Modem/VNPT.
---	--	----	--

6.2.1.3 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 tổ chức	Có	Hệ thống được thiết lập chính sách chỉ cho phép truy cập ra bên ngoài với các dịch vụ phổ biến, phục vụ hoạt động nghiệp vụ bao gồm: TCP 80,443,25,587,...;UDP 53, 123,...

6.2.1.4. Nhật ký hệ thống

Yêu cầu	Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống
Thiết bị	
Modem/VNPT	+
DrayTek Vigor2920FV Fiber router	+
SWDMZ/Cisco2960	+
SWSF/ Cisco2960	+
SW/Cisco2960	+
SW L2/Cisco2960	+
WAF/WAF v2secure	+

6.2.1.5. 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 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	Đáp ứng	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.

6.2.1.6. Bảo vệ thiết bị hệ thống

Yêu cầu	Cấu hình chức năng xác thực trên các thiết bị	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa	Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa
Thiết bị			
Modem/VNPT	+	+	+
DrayTek Vigor2920FV Fiber router	+	+	+
SWSF/ Cisco2960	+	+	+
SW/Cisco2960	+	+	+
SWL2/Cisco2960	+	+	+

6.2.2. Bảo đảm an toàn máy chủ

6.2.2.1. Xác thực

Yêu cầu	Thiết lập chính sách xác thực	Thay đổi các tài khoản mặc định	Thiết lập chính sách mật khẩu an toàn: Yêu cầu thay đổi mật khẩu mặc định; Thiết lập quy tắc đặt
---------	-------------------------------	---------------------------------	--

Máy chủ	trên máy chủ	định trên hệ thống hoặc vô hiệu hóa	mật khẩu về số ký tự, loại ký tự; Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ
Trang thông tin điện tử tổng hợp: Cấu hình máy chủ ảo: CPU 8 core; Ram 16G; ổ cứng 200G. Công nghệ website: Nukeviet 3.0 Database: MariaDB Tên miền: dakglong.daknong.gov.vn (IP: 103.147.100.138) Đặt tại Trung tâm Dữ liệu Công nghệ và Truyền thông tỉnh Đắk Nông	+	+	+

6.2.2.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)
Máy chủ		
Trang thông tin điện tử tổng hợp: Cấu hình máy chủ ảo: CPU 8 core; Ram 16G; ổ cứng 200G. Công nghệ website: Nukeviet 3.0 Database: MariaDB Tên miền: dakglong.daknong.gov.vn	+	+

(IP: 103.147.100.138) Đặt tại Trung tâm Dữ liệu Công nghệ và Truyền thông tỉnh Đắk Nông		
--	--	--

6.2.2.3. Nhật ký hệ thống

Yêu cầu	Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ	Đồng bộ thời gian giữa máy chủ với máy chủ thời gian	Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng
Máy chủ			
Trang thông tin điện tử tổng hợp: Cấu hình máy chủ ảo: CPU 8 core; Ram 16G; ổ cứng 200G. Công nghệ website: Nukeviet 3.0 Database: MariaDB Tên miền: dakglong.daknong.gov.vn (IP: 103.147.100.138) Đặt tại Trung tâm Dữ liệu Công nghệ và Truyền thông tỉnh Đắk Nông	+	+	+

6.2.2.4. Phòng chống xâm nhập

Yêu cầu	Loại bỏ các tài khoản không sử dụng, các	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm	Vô hiệu hóa các giao thức mạng không an toàn, các	Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên
Máy chủ				

	tài khoản không còn hợp lệ trên máy chủ	các truy cập trái phép tới máy chủ	dịch vụ hệ thống không sử dụng	máy chủ trước khi đưa vào sử dụng
Trang thông tin điện tử tổng hợp: Cấu hình máy chủ ảo: CPU 8 core; Ram 16G; ổ cứng 200G. Công nghệ website: Nukeviet 3.0 Database: MariaDB Tên miền: dakglong.daknong.gov.vn (IP: 103.147.100.138) Đặt tại Trung tâm Dữ liệu Công nghệ và Truyền thông tỉnh Đắk Nông	+	+	+	+

6.2.2.5. Phòng chống phần mềm độc hại

Yêu cầu	Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật	Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt
Máy chủ		
Trang thông tin điện tử tổng hợp: Cấu hình máy chủ ảo: CPU 8 core; Ram 16G; ổ cứng 200G. Công nghệ website: Nukeviet 3.0 Database: MariaDB Tên miền: dakglong.daknong.gov.vn (IP: 103.147.100.138) Đặt tại Trung tâm Dữ liệu Công nghệ và Truyền thông tỉnh Đắk Nông	+	+

6.2.2.6. Xử lý máy chủ khi chuyển giao

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	Đáp ứng	Hiện tại chưa có phương án chuyển giao cho đơn vị sử dụng. Sẽ có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng

6.2.3. Bảo đảm an toàn ứng dụng

6.2.3.1. Xác thực

Yêu cầu	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
Ứng dụng				
Trang thông tin điện tử huyện Đắk Glong. Tên miền: dakglong.daknong.gov.vn (IP: 103.147.100.138)	+	+	+	+

6.2.3.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa
Ứng dụng			
Trang thông tin điện tử huyện Đắk Glong.	+	+	+

6.2.3.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng.	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng
Ứng dụng		
Trang thông tin điện tử huyện Đắk Glong.	+	+

6.2.3.4. An toàn ứng dụng và mã nguồn

Yêu cầu	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
Ứng dụng	
Trang thông tin điện tử huyện Đắk Glong.	+

6.2.4. Bảo đảm an toàn dữ liệu

6.2.4.1 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	Có	Dữ liệu được nén và thiết lập mật khẩu để bảo vệ. Tập tin lưu trữ phải có mã kiểm tra tính toàn vẹn kèm theo.
---	---	----	---

6.2.4.2 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	Có	Định kỳ thành tháng 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.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Đoàn Văn Phương