UBND TỈNH HÀ GIANG **SỞ TƯ PHÁP**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 152 /QĐ-STP	*Hà Giang, ngày 21 tháng 11 năm 2023*

QUYẾT ĐỊNH
Về việc phê duyệt hồ sơ cấp độ an toàn thông tin

GIÁM ĐỐC SỞ TƯ PHÁP TỈNH HÀ GIANG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về việc bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12/8/2023 của Bộ Thông tin và Truyền thông về việc quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Quyết định số 23/2021/QĐ-UBND ngày 12 tháng 8 năm 2021 của Ủy ban nhân dân Hà Giang quy định cụ thể chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Tư pháp Hà Giang;

Theo đề nghị của Chánh văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt hồ sơ cấp độ an toàn thông tin mạng LAN.

(Kèm theo hồ sơ đề xuất cấp độ an toàn thông tin)

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Giao Văn phòng Sở thực hiện đảm bảo an toàn hệ thống thông tin được giao quản lý theo quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP; ban hành phương án bảo đảm an toàn thông tin và tổ chức vận hành theo quy định.

Điều 3. Chánh Văn phòng Sở, Trưởng các Phòng, Đơn vị thuộc và trực thuộc Sở, các cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Sở TTTT;
- Lãnh đạo Sở;
- Trang TTĐT của Sở;
- Lưu: VT, VP, ĐT 02.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ TƯ PHÁP
TỈNH HÀ GIANG

Trương Huy Huân

UBND TỈNH HÀ GIANG
SỞ TƯ PHÁP

HỒ SƠ
CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN MẠNG LAN

Hà Giang, năm 2023

MỤC LỤC

THUẬT NGỮ, TỪ VIẾT TẮT

STT	Từ viết tắt	Giải thích
1	STP	Sở Tư pháp
2	CNTT	Công nghệ thông tin
3	TTĐT	Thông tin điện tử
4	Firewall	Tường lửa

DANH MỤC CÁC BẢNG

DANH MỤC CÁC HÌNH VẼ

Phần I
THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

1. Thông tin Chủ quản hệ thống thông tin

- Tên cơ quan: Sở Tư pháp tỉnh Hà Giang.
- Người đại diện: Giám đốc Sở Tư pháp .
- Địa chỉ: Đường Trần Quốc Toản, phường Nguyễn Trãi, thành phố Hà Giang, tỉnh Hà Giang.
- Thông tin liên hệ:

+ Điện thoại: 02193. 866 415

+ Email: stp@hagiang.gov.vn.

2. Thông tin đơn vị vận hành

- Tên đơn vị vận hành: Văn Phòng Sở.
- Người đại diện: Chánh Văn Phòng, vai trò: phụ trách điều hành hệ thống.
- Email: vp.stp@hagiang.gov.vn.

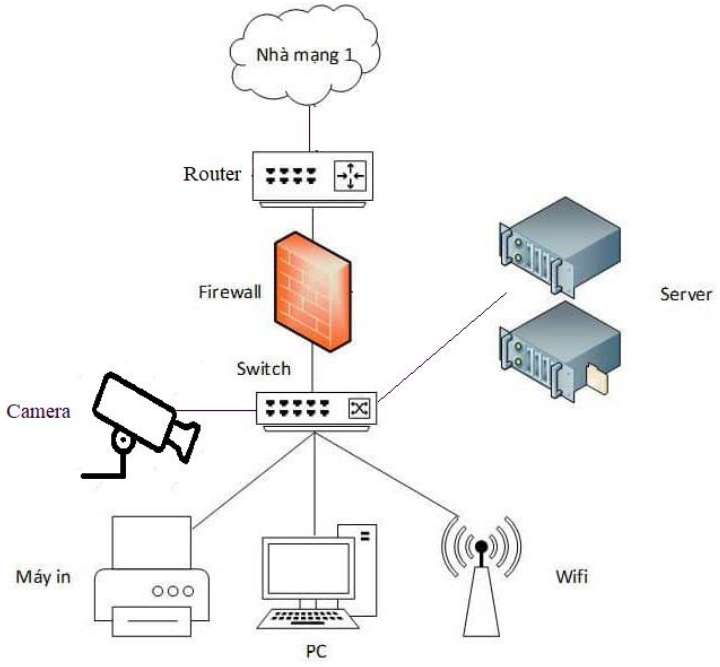
3. Mô tả phạm vi, quy mô của hệ thống

Hệ thống thông tin (mạng LAN) phục vụ hoạt động nội bộ cơ quan được thiết lập để phục vụ việc truy cập internet và chia sẻ các tài nguyên trên hệ thống.

- Đối tượng phục vụ của hệ thống: Công chức, viên chức, người lao động thuộc Sở Tư pháp tỉnh Hà Giang, dưới 100 người.
- Danh mục các dịch vụ được cung cấp bởi hệ thống: LAN.

4. Mô tả cấu trúc của hệ thống

4. 1. Sơ đồ logic tổng thể



Hình 1: Cấu trúc logic của Hệ thống thông tin phục vụ hoạt động nội bộ cơ quan

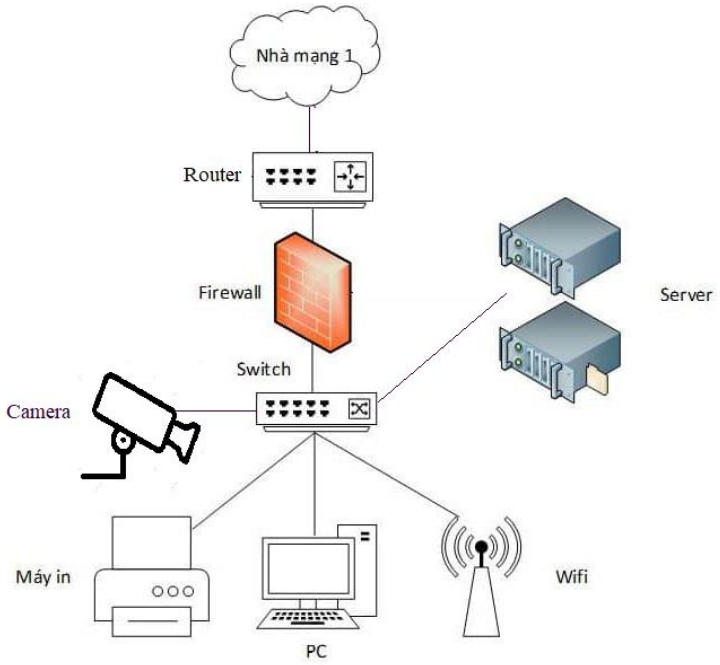
- Các vùng mạng được thiết kế như sau:

+ Vùng mạng biên được thiết kế để kết nối hệ Hệ thống thông tin phục vụ

hoạt động nội bộ ra các mạng bên ngoài và mạng Internet;

+ Vùng mạng nội bộ để kết nối các máy tính của người sử dụng.

4.2. Sơ đồ kết nối vật lý



Hình 2: Kết nối vật lý của Hệ thống thông tin phục vụ hoạt động nội bộ

4.3. Danh mục các thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Router	Vùng mạng biên	Kết nối và định tuyến động với các Router của 01 ISP
2	PC	Vùng mạng nội bộ	Máy trạm

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

- Quy hoạch địa chỉ IP tĩnh theo từng phòng, ban chuyên môn để hạn chế trùng địa chỉ IP, cụ thể như sau:

STT	Địa chỉ IP	Vị trí triển khai	Mục đích sử dụng
1	Dải IP của cơ quan		- Kết nối mạng Internet - Cung cấp kết nối cho các máy trạm

- Quy hoạch địa chỉ IP cho hệ thống Wifi riêng để không ảnh hưởng đến dãy IP trong hệ thống.

STT	Địa chỉ IP	Vị trí triển khai	Mục đích sử dụng
1	Dải IP Wifi của cơ quan		Cung cấp kết nối Wifi cho các thiết bị

Phần II
THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

Hệ thống thông tin thuộc phạm vi quản lý của Sở Tư pháp bao gồm các hệ thống thông tin với cấp độ đề xuất tương ứng, bao gồm:

TT	Hệ thống	Loại thông tin xử lý	Loại hình HTTT	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống mạng nội bộ (LAN)	Thông tin công cộng, thông tin riêng của tổ chức	Hệ thống thông tin phục vụ hoạt động nội bộ	2	Khoản 1 Điều 8 Nghị định số 85

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

Hệ thống mạng LAN nội bộ cơ quan phục vụ hoạt động của cơ quan: Trao đổi, quản lý, chỉ đạo, diều hành, xử lý công việc trên môi trường điện tử; gửi, nhận văn bản điện tử với UBND tỉnh, các sở, ban, ngành, UBND cấp huyện và các đơn vị sự nghiệp trực thuộc. Căn cứ theo quy định tại Khoản 3 Điều 8 Nghị định 85/2016/NĐ-CP. Hệ thống này được đề xuất cấp độ 2.

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.

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 trong 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 dữ liệu.

2.1. 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.

Căn cứ vào nội dung thuyết minh đề xuất cấp độ ở Mục 2, Phần 2. Thuyết minh phương án bảo đảm an toàn thông tin về quản lý đưa ra các quy định liên quan đến con người và quy trình. Các yêu cầu đối với phương án được thể hiện một phần trong Quy chế bảo đảm an toàn thông tin. Đối với những yêu cầu chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, Đơn vị vận hành sẽ tham mưu hoàn thiện trong quy chế, chính sách để đáp ứng yêu cầu.

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho hệ thống thông tin sẽ bao gồm các thuyết minh thành phần sau:

I. THUYẾT MINH PHƯƠNG ÁN VỀ QUẢN LÝ

1. Mục tiêu, nguyên tắc về bảo đảm an toàn thông tin

- Đảm bảo tính bí mật của thông tin, tức là thông tin chỉ được phép truy cập bởi những đối tượng được cấp phép.

- Đảm bảo tính toàn vẹn của thông tin, tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi.

- Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.

- Nguyên tắc bảo đảm an toàn thông tin phải tuân thủ các nguyên tắc tại Điều 4 của Luật An toàn thông tin và Điều 4 của Nghị định số 85/2016/NĐ-CP.

- Tất cả các phòng ban, đơn vị có trách nhiệm bảo đảm an toàn thông tin của đơn vị mình theo đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước.

- Được thực hiện thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ; tuân thủ theo các tiêu chuẩn, quy chuẩn kỹ thuật được các cơ quan chức năng ban hành.

- Nhận biết, phân loại, đánh giá kịp thời và xử lý có hiệu quả các rủi ro an toàn thông tin mạng có thể xảy ra trong cơ quan, đơn vị.

- Xây dựng, triển khai quy chế an toàn thông tin trên cơ sở hài hòa giữa lợi ích, chi phí và mức độ chấp nhận rủi ro của đơn vị.

- Sở đã có 01 biên chế chuyên trách CNTT tham mưu giúp Giám đốc Sở thực hiện quản lý, vận hành, sử dụng cơ sở hạ tầng thông tin phục vụ hoạt động quản lý, điều hành của Sở; đảm bảo kỹ thuật, an toàn hệ thống thông tin, cơ sở dữ liệu thuộc lĩnh vực quản lý của ngành; thực hiện ứng dụng CNTT trong công bố, công khai, minh bạch và giải quyết thủ tục hành chính.

- Xác định rõ quyền hạn, trách nhiệm của Thủ trưởng cơ quan, đơn vị (hoặc người đại diện hợp pháp), từng bộ phận và cá nhân trong cơ quan, đơn vị đối với công tác bảo đảm an toàn thông tin mạng.

2. Trách nhiệm bảo đảm an toàn thông tin

- Quy định trách nhiệm của phòng, ban chuyên môn, các đơn vị sự nghiệp trực thuộc sử dụng chung hệ thống mạng LAN tại Cơ quan trong công tác bảo đảm an toàn thông tin.

- Ban hành Quy chế bảo đảm an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của Sở Tư pháp .

3. Phạm vi chính sách an toàn thông tin

Yêu cầu	Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin
Phương án	1. Mục tiêu: Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin. 2. Nguyên tắc bảo đảm an toàn thông tin: a) Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội. b) Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác. c) Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức. d) Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.
Yêu cầu	Xác định trách nhiệm của các Lãnh đạo Sở, các Phòng, Đơn vị thuộc và trực thuộc Sở, các công chức làm về an toàn thông tin và

	các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin
Phương án	Quy định trách nhiệm của các Lãnh đạo Sở, các Phòng, Đơn vị trong công tác bảo đảm an toàn thông tin: 1. Trách nhiệm của Lãnh đạo Sở - Chịu trách nhiệm trước Chủ tịch UBND tỉnh về công tác bảo đảm an toàn thông tin mạng trong nội bộ cơ quan Sở và các đơn vị trực thuộc. - Sở Tư pháp có trách nhiệm thực hiện các nhiệm vụ của chủ quản hệ thống thông tin đối với các hệ thống thông tin trong phạm vi cơ quan Sở theo quy định tại Điều 20, Nghị định 85. - Phân công một bộ phận hoặc cán bộ phụ trách bảo đảm an toàn thông tin mạng của đơn vị, tạo điều kiện để các cán bộ được học tập, nâng cao trình độ về an toàn thông tin mạng. - Bố trí, tạo điều kiện làm việc cho cán bộ chuyên trách về công nghệ thông tin trong các cơ quan, đơn vị phù hợp với chuyên môn, được ưu tiên bồi dưỡng nghiệp vụ về an toàn thông tin mạng. 2. Trách nhiệm của Văn phòng Sở: a) Tham mưu lãnh đạo cơ quan tổ chức thực thi, đôn đốc, giám sát công tác đảm an toàn thông tin trong hệ thống thông tin nội bộ tại cơ quan, ngành theo quy định tại Điều 21, Nghị định 85/2016/NĐ-CP. c) Đảm bảo vận hành tốt đối với hệ thống thông tin thuộc phạm vi quản lý. d) Hàng năm cử cán bộ chuyên trách quản trị mạng tham gia các chương trình đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng do các sở, ban ngành cấp tỉnh tổ chức. e) Tổ chức tuyên truyền, hướng dẫn về công tác bảo đảm an toàn thông tin mạng trên các phương tiện thông tin đại chúng và trên Trang TTĐT của cơ quan. f) Hàng năm lập dự toán kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan; lập kế hoạch nâng cấp, bảo trì, sửa chữa, cài đặt phần mềm diệt virus bản quyền... Đề xuất sửa chữa, nâng cấp, thay thế trang thiết bị không phù hợp để đảm bảo an toàn thông tin trong toàn hệ thống. g) Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo quy định của pháp luật. 3. Trách nhiệm của công chức, viên chức và người lao động trong các cơ quan

	a) Trách nhiệm lãnh đạo các Phòng, Đơn vị thuộc và trực thuộc - Chịu trách nhiệm bảo đảm an toàn thông tin mạng của Phòng, Đơn vị mình quản lý. - Trưởng các Phòng, Đơn vị chỉ đạo công chức, viên chức, người lao động của Phòng, Đơn vị mình thực hiện nghiêm các quy định bảo bảo an toàn thông tin trong toàn hệ thống mạng LAN cơ quan, không sử dụng các thiết bị ngoại vi để sao chép, chia sẻ thông tin, dữ liệu. - Nâng cao ý thức trách nhiệm của công chức, viên chức, người lao động thuộc Phòng, Đơn vị về đảm bảo an toàn thông tin trong hệ thống mạng LAN cơ quan. - Phối hợp với phòng trong công tác kiểm tra, phát hiện, xử lý kịp thời các sự cố về an toàn thông tin mạng. b) Trách nhiệm của người sử dụng: - Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin 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 an toàn thông tin mạng phải báo cáo ngay với cấp trên và công chức chuyên trách CNTT của cơ quan để kịp thời ngăn chặn và xử lý; - Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức. c) Trách nhiệm của công chức chuyên trách CNTT - Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nội bộ cơ quan. - Chủ trì, phối hợp với Phòng, 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 cấp trên hoặc các cơ quan chuyên môn. - Tùy theo mức độ sự cố, phối hợp tham mưu cho sở, Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh và các đơn vị có liên quan xử lý, ứng cứu các sự cố an toàn thông tin mạng. - Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ.

3.2. Xây dựng và công bố

Yêu cầu	Quy định về xây dựng và công bố Quy chế bảo đảm an toàn thông tin

Phương án	Xây dựng và công bố Quy chế bảo đảm an toàn thông tin: 1. Quy chế được lấy ý kiến cấp có thẩm quyền, đơn vị liên quan trước khi công bố áp dụng 2. Quy chế được xây dựng trình Giám đốc Sở ban hành.

3.3. Rà soát, sửa đổi

Yêu cầu	Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin
Phương án	Rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin: 1. Định kỳ 02 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin do UBND tỉnh ban hành sẽ 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 Phòng, Đơn vị phản ánh kịp thời về Văn phòng Sở để tổng hợp báo cáo Lãnh đạo Sở điều chỉnh, bổ sung.

4. Tổ chức bảo đảm an toàn thông tin

4.1. Đơn vị chuyên trách về an toàn thông tin

Yêu cầu	Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về an toàn thông tin trong tổ chức
Phương án	- Giao Văn phòng Sở là đơn vị chuyên trách về an toàn thông tin, trình Giám đốc Sở ban hành Quyết định. - Văn phòng Sở dự thảo Quyết định trình giám đốc Sở giao nhiệm vụ cho bộ phận chuyên trách về an toàn thông tin.

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

Yêu cầu	Có quy định về việc phối hợp với những cơ quan/tổ chức có thẩm quyền
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) Giám đốc Sở giao cho công chức chuyên trách CNTT là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin. b) Công chức chuyên trách CNTT làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong phạm vi của ngành.

Phương án	c) Văn phòng Sở chủ trì, Đội ứng cứu sự cố của tỉnh 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 Đội ứng cứu sự cố của tỉnh hoặc và các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

5. Bảo đảm nguồn nhân lực

5.1. Tuyển dụng

Yêu cầu	Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ
Phương án	Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ: 1. Quy định cán bộ được giao nhiệm vụ 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 việc làm. 2. Xây dựng yêu cầu về vị trí việc làm về CNTT

5.2. 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
Phương án	Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc: 1. 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 - 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. 2. Tổ chức phổ biến, tuyên truyền nâng cao nhận thức cho cán bộ, công chức, viên chức và người lao động về an toàn thông tin.

5.3. Chấm dứt hoặc thay đổi công việc

Yêu cầu	Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc
Phương án	Quy định đối với cán bộ nghỉ hoặc thay đổi công việc: 1. Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thông tin tài khoản 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 chứ. 2. Cán bộ quản trị phải vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc. 3. Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

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

6.1. Thiết kế an toàn hệ thống thông tin

Yêu cầu	Có quy định về thiết kế an toàn hệ thống thông tin
Phương án	Quy định đối với tài liệu thiết kế hệ thống: 1. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin. 2. Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin. 3. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. 4. Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. 5. 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.

6.2. Phát triển phần mềm thuê khoán

Yêu cầu	Có quy định về phát triển phần mềm thuê khoán
Phương án	Quy định đối với việc phát triển phần mềm thuê khoán: 1. Có điều khoản hợp đồng và các cam kết đối với bên thuê khoán khi thực hiện các nội dung liên quan đến việc phát triển phần mềm thuê khoán. 2. Các nhà phát triển cung cấp mã nguồn phần mềm.

	3. Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng. 4. Phần mềm thuê khoán phải được kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

6.3. Thử nghiệm và nghiệm thu hệ thống

Yêu cầu	Có quy định về việc thử nghiệm và nghiệm thu hệ thống
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. 3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống. 4. Có 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. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.

7. Quản lý vận hành hệ thống thông tin

7.1. Quản lý an toàn mạng

Yêu cầu	Có quy định về quản lý an toàn mạng
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 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. 3. Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa; Hạn chế được số lần đăng nhập sai; Phân quyền truy cập, quản trị; Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng.

	4. Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công; triển khai cơ chế phòng chống vi rút tin học tại các máy trạm khác trong hệ thống. 5. Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng phải đảm bảo yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy. 6. Đối với các thiết bị mạng chính a) Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT, phải xây dựng ít nhất 02 thiết bị chống sét: một cho một đường cung cấp điện và một đường của mạng nội bộ (LAN). c) Thiết bị chuyển mạch (switch): Thiết bị chuyển mạch mạng tin học của các cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: cung cấp khả năng từ chối các kết nối không mong muốn vào hệ thống trên từng cổng, quy định địa chỉ IP cho từng cổng và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch có hỗ trợ định tuyến IP (IP routing) cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập (Access Control List), hỗ trợ chức năng xác thực thiết bị và người sử dụng (User & Device Authentication) và chức năng bảo mật quản trị mạng (Network Administration Security). 7. Tệp tin cấu hình, sơ đồ mạng logic và vật lý phải được cập nhật, sao lưu dự phòng. 8. 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 hệ thống sau thảm họa.

7.2. Quản lý an toàn dữ liệu

Yêu cầu	Có quy định về quản lý an toàn dữ liệu
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. 3. 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.

7.4. Quản lý an toàn thiết bị đầu cuối

Yêu cầu	Có quy định về quản lý thiết bị đầu cuối
Phương án	Các thiết bị đầu cuối khi kết nối và hệ thống phải được quản lý như sau: 1. Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật. 2. Các thiết bị đầu cuối phải được quản lý khi kết nối vào hệ thống mạng theo địa chỉ MAC, IP.
	3. Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn. 4. Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.

7.8. Quản lý sự cố an toàn thông tin

Yêu cầu	Có quy định về quản lý sự cố an toàn thông tin
Phương án	Quy định về quản lý sự cố an toàn thông tin: 1. Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm: a) Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng. b) Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng. c) Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05. d) Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo. e) 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; Yêu cầu bên cung cấp, hỗ trợ cung cấp quy trình xử lý sự cố cho các dịch vụ do bên cung cấp, hỗ trợ cung cấp liên quan đến

	hệ thống. g) Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. 2. Trách nhiệm của người dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

7.9. Quản lý an toàn người sử dụng đầu cuối

Yêu cầu	Có quy định về quản lý an toàn người sử dụng đầu cuối
Phương án	Quy định về quản lý an toàn người sử dụng đầu cuối: 1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống: a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin 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 an toàn thông tin. 2. Trong quá trình sử dụng: a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao; b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý; d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

II. THUYẾT MINH PHƯƠNG ÁN VỀ KỸ THUẬT

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

STT	Yêu cầu	Phương án	Ghi chú/Mô tả

1	Vùng mạng nội bộ	Có	Vùng mạng cung cấp cho các máy trạm trong cơ quan Sở có kết nối với internet
2	Vùng mạng biên	Có	Kết nối hệ thống với mạng Internet
3	Vùng mạng không dây	Có	Cấu hình riêng dạng Meesh đảm bảo cân bằng tải khi truy cập và khai thác hệ thống

1.2 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	Chưa có	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 hệ thống firewall.

1.3. Nhật ký hệ thống

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Xây dựng cơ chế kiểm soát, sao lưu nhật ký hệ thống.	Có	Hệ thống nhật ký hiện mới chỉ bật tính năng trên thiết bị Router; các thiết bị mạng khác chưa có chức năng này.

1.4. Phòng chống xâm nhập

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống	Chưa có	Các vùng mạng được triển khai hệ thống IDS/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	Chưa 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 IDS/IPS.

1.5. Bảo vệ thiết bị hệ thống

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Cấu hình thiết bị chỉ cho phép hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa	Có	Đã thiết lập chức năng trên thiết bị Router

2. Bảo đảm an toàn dữ liệu

2.1. Sao lưu dự phòng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu 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	- Thực hiện sao lưu các dữ liệu quan trọng của cơ quan tại các vị trí như văn thư, kế toán, tổ chức cán bộ…sang các thiết bị lưu trữ độc lập. - Hệ thống sao lưu dự phòng NAS: cho phép tạo lập thư mục và chia sẻ dữ liệu trong nội bộ LAN của Sở.