UBND TỈNH TUYÊN QUANG
SỞ NỘI VỤ

Số: 241/QĐ-SNV

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Tuyên Quang, ngày 31 tháng 12 năm 2022

QUYẾT ĐỊNH
Về việc phê duyệt cấp độ an toàn hệ thống thông tin Hệ thống mạng nội bộ Sở Nội vụ

GIÁM ĐỐC SỞ NỘI VỤ

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

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

Căn cứ Quyết định số 05/2022/QĐ-UBND ngày 30 tháng 3 năm 2022 của Ủy ban nhân dân tỉnh quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Nội vụ tỉnh Tuyên Quang;

Theo đề nghị của Chánh Văn phòng Sở.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống mạng nội bộ (mạng LAN) Sở Nội vụ, cụ thể như sau:

1. Thông tin chung

a) Tên hệ thống thông tin: Hệ thống mạng nội bộ (mạng LAN) Sở Nội vụ.

b) Đơn vị vận hành hệ thống thông tin: Văn phòng Sở.

c) Đơn vị quản lý: Sở Nội vụ.

- Địa chỉ: Số 01, đường Lý Thánh Tông, phường Minh Xuân, thành phố Tuyên Quang, tỉnh Tuyên Quang.

2. Cấp độ an toàn hệ thống thông tin: Hệ thống thông tin cấp độ 1.

3. Phương án bảo đảm an toàn thông tin:

a) Phương án bảo đảm an toàn thông tin trong thiết kế hệ thống thông tin tương ứng với cấp độ 1 là phù hợp với tiêu chuẩn quốc gia (TCVN 11930:2017), quy chuẩn kỹ thuật quốc gia (TCVN 11930:2017) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

b) Phương án bảo đảm an toàn thông tin trong quá trình vận hành hệ thống tương ứng với cấp độ 1 là phù hợp với tiêu chuẩn quốc gia (TCVN 11930:2017), quy chuẩn kỹ thuật quốc gia (TCVN 11930:2017) về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 2. Văn phòng Sở chịu trách nhiệm:

1. Kiểm tra, giám sát đảm bảo an toàn mạng nội bộ LAN của Sở Nội vụ theo cấp độ 1 được quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính Phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Vận hành mạng nội bộ LAN của Sở Nội vụ đảm bảo các yêu cầu theo quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính Phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Điều 3. Điều khoản thi hành

Văn phòng Sở, các đơn vị thuộc Sở và các cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3 (thực hiện);
- UBND tỉnh (báo cáo);
- Sở Thông tin và Truyền thông;
- Giám đốc Sở;
- Phó Giám đốc Sở;
- Các đơn vị thuộc Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ NỘI VỤ
TỈNH TUYÊN QUANG

Vũ Quang Thắng

SỞ NỘI VỤ TỈNH TUYÊN QUANG
VĂN PHÒNG

HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 1
HỆ THỐNG MẠNG NỘI BỘ (MẠNG LAN)
CỦA SỞ NỘI VỤ

Tuyên Quang, năm 2022

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: Sở Nội vụ Tuyên Quang

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 05/2022/QĐ-UBND ngày 30/3/2022 của Ủy ban nhân dân tỉnh quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Nội vụ tỉnh Tuyên Quang.

- Người đại diện: Vũ Quang Thắng, Chức vụ: Giám đốc Sở.

- Địa chỉ: Số 01, đường Lý Thánh Tông, phường Minh Xuân, thành phố Tuyên Quang, tỉnh Tuyên Quang.

- Thông tin liên hệ: Điện thoại: 02073822432 - Email: noivu@tuyenquang.gov.vn

2. Thông tin đơn vị vận hành

- Tên đơn vị vận hành: Văn phòng Sở.

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 86/QĐ-SNV ngày 10/5/2022 của Sở Nội vụ quy định chức năng, nhiệm vụ, quyền hạn của các tổ chức, cơ quan, đơn vị thuộc và trực thuộc Sở Nội vụ.

- Người đại diện: Ông Lê Quốc Huân, Chức vụ: Chánh Văn phòng sở.

- Địa chỉ: Số 01, đường Lý Thánh Tông, phường Minh Xuân, thành phố Tuyên Quang, tỉnh Tuyên Quang.

- Thông tin liên hệ: Điện thoại: 02073817500

3. Mô tả phạm vi, quy mô của hệ thống

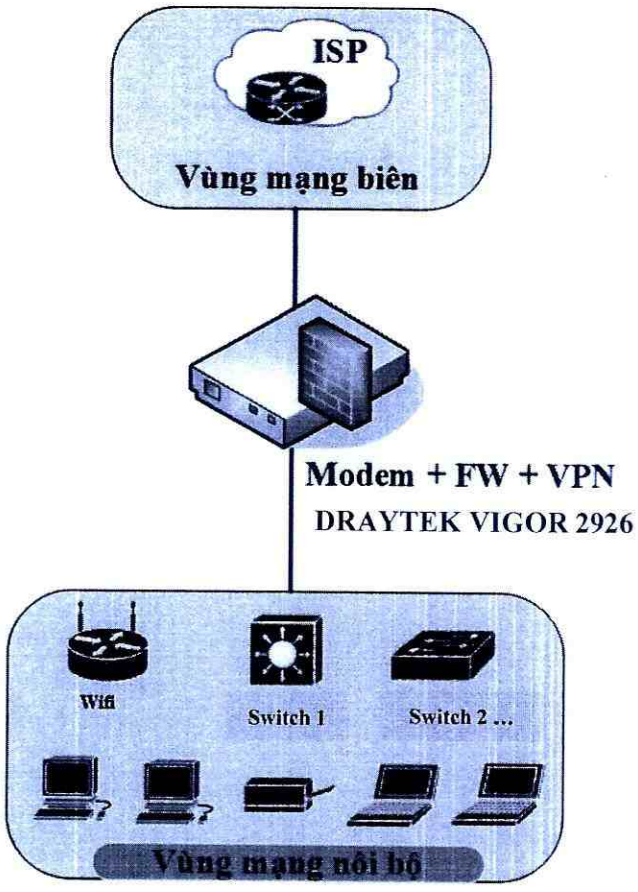
- Phạm vi, quy mô của Hệ thống Mạng LAN: Hệ thống thông tin của Sở Nội vụ được thiết lập để phục vụ công tác chỉ đạo, điều hành và hoạt động trong phạm vi Sở Nội vụ.

- Đối tượng phục vụ của hệ thống: Công chức, người lao động làm việc tại các đơn vị thuộc Sở.

- Danh mục các hệ thống thông tin thành phần: Hệ thống Mạng LAN.

4. Mô tả cấu trúc của hệ thống

4.1. Mô hình logic tổng thể



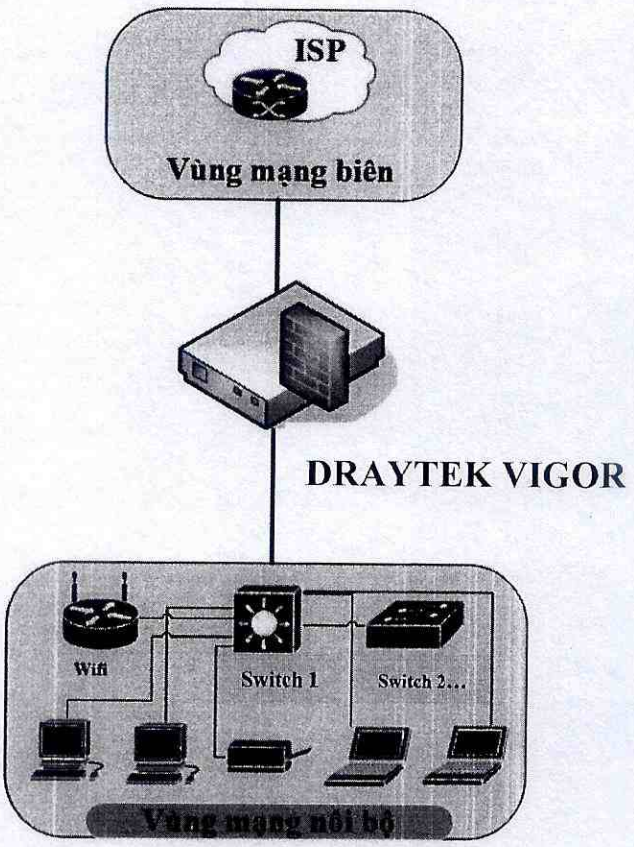
Hình 1. Cấu trúc logic của hệ thống

Các vùng mạng được thiết kế như sau:

+ Vùng mạng biên được thiết kế để kết nối hệ thống ra các mạng bên ngoài và mạng Internet.

+ Vùng mạng nội bộ đặt các thiết bị nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống.

4.2. Mô hình kết nối vật lý



Hình 2. Kết nối vật lý của hệ thống

4.3. Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	DRAYTEK VIGOR	Vùng mạng biên	Kết nối và định tuyến động với các Router của ISP.
3	Switch TpLink 1	Vùng mạng nội bộ	Chuyển mạch trung tâm đảm bảo tốc độ vận chuyển và liên kết với các lớp mạng
4	Switch TpLink 2	Vùng mạng nội bộ	Thiết bị định tuyến vùng mạng nội bộ
5	Wifi TPlink	Vùng mạng nội bộ	Thiết bị cung cấp kết nối internet không dây cho vùng mạng nội bộ

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

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

STT	Tên dịch vụ	Máy chủ/Ứng dụng cài đăt/Vùng mạng/HĐH	Mục đích sử dụng
1	Hệ thống Mạng LAN	Vùng mạng	Cung cấp thông tin công khai cho người sử dụng nội bộ.

Bảng 2. 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 mạng nội bộ	192.168.1.0/24	221.132.2.152

Bảng 3. 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 mạng nội bộ (mạng LAN) của Sở Nội vụ bao gồm hệ thống thành phần với cấp độ đề xuất tương ứng như sau:

STT	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống mạng LAN	1	Điều 7/NĐ85

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

Hệ thống Mạng LAN chỉ xử lý thông tin công khai và phục vụ hoạt động nội bộ cho công chức của Sở Nội vụ. Căn cứ theo quy định tại Điều 7/NĐ85, hệ thống này được đề xuất cấp độ 1.

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

Thuyết minh phương án về quản lý bao gồm các nội dung sau:

1. Thiết lập chính sách an toàn thông tin

2. Tổ chức bảo đảm an toàn thông tin

3. Bảo đảm nguồn nhân lực

4. Quản lý 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

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: Có thuyết minh đáp ứng khi có 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: Có thuyết minh đáp ứng khi có 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 18 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống mạng LAN của Sở Nội vụ 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	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	Đơn vị vận hành xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống (*Quyết định 240/QĐ-SNV ngày 31/12/2022 về ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ)*
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: **Hệ thống mạng LAN không có máy chủ và ứng dụng.** 3. Quản lý an toàn dữ liệu: **Hệ thống mạng LAN không có Quản lý dữ liệu.** 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. g) 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	Xây dựng, công bố Quy chế bảo đảm an toàn thông tin *(Quyết định 240/QĐ-STTTT, ngày 31/12/2022 về ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ)*
Phương án	Chính sách được tổ chức/ bộ phận được ủy quyền thông qua trước khi công bố áp dụng Xây dựng và công bố Quy chế bảo đảm an toàn thông tin: Quy chế được Sở Nội vụ xây dựng ban hành.

5.1.1.3. Rà soát, sửa đổi

Yêu cầu	Chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.
Hiện trạng	Đáp ứng. Tham chiếu Điều 7 Quy chế bảo đảm an toàn, an ninh

	thông tin mạng Sở Nội vụ
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 Nội vụ để tổng hợp 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. Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ
Phương án	Sở Nội vụ giao Văn phòng Sở là đơn vị chuyên trách về an toàn thông tin thực hiện 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. Tham chiếu Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ
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) Sở Nội vụ giao Văn phòng Sở là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin. b) Văn phòng Sở làm đầu mối, tổ chức thực hiện việc tiếp nhận

	và xử lý các sự cố về an toàn thông tin mạng. c) Văn phòng Sở chủ trì, phối hợp với các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm. 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 với Sở Thông tin và Truyền thông, 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. Tham chiếu Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ.
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 (Văn phòng Sở)

5.1.3. Bảo đảm nguồn nhân lực

5.1.3.1. Tuyển dụng

Yêu cầu	Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng.
Hiện trạng	Đáp ứng. Tham chiếu Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ.
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. Tham chiếu Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ.
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 công chức quản lý và vận hành hệ thống - Công chức 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. - Công chức 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. Tham chiếu Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ.
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	Công chức chấm dứt hoặc thay đổi công việc phải thu hồi 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 (nếu có) thuộc sở hữu của tổ chức.
Hiện trạng	Đáp ứng. Tham chiếu khoản 4, Điều 7 Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ.
Phương án	Quy định đối với công chức nghỉ hoặc thay đổi công việc: a) Công chức nghỉ hoặc thay đổi công việc phải thu hồi 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 chức. b) Vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi công chức 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. Trình bày tại Hồ sơ cấp độ
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. Trình bày tại Hồ sơ cấp độ
Phương án	Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.

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. Tham chiếu Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ.
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: *Hệ thống mạng LAN không sử dụng máy chủ và ứng dụng.*

Yêu cầu	Xây dựng và thực thi chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ.
Hiện trạng	Hệ thống mạng LAN không sử dụng máy chủ và ứng dụng.
Phương án	Hệ thống mạng LAN không sử dụng máy chủ và ứng dụng.

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	Hệ thống mạng LAN không lưu trữ dữ liệu.
Phương án	Hệ thống mạng LAN không sử dụng máy chủ và ứng dụng.

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. Tham chiếu Điều 9 Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ; Quyết định số 97/QĐ-SNV ngày 27/12/2016 của Sở Nội vụ về ban hành quy trình xử lý sự cố, lỗ hổng và phương án, giải pháp kỹ thuật đảm bảo an toàn thông tin, an ninh mạng của Sở Nội vụ.
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. Tham chiếu Điều 3 Quy chế bảo đảm an toàn, an ninh thông tin mạng Sở Nội vụ.
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 của Sở Nội vụ. Căn cứ theo quy định tại Điều 7, Nghị định số 85, 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: *(Hệ thống đáp ứng khi có máy chủ)*

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 tường lửa Firewall01 có tích hợp tính năng VPN quản lý truy cập, quản trị hệ thống từ xa an toàn. Tính năng VPN này được cấu hình trực tiếp trên thiết bị Firewall01, quản lý truy cập từ bên ngoài vào vùng mạng nội bộ
2	Phương án quản lý truy cập giữa các	Có	Truy cập giữa các vùng mạng được quản lý và phòng chống xâm nhập sử dụng

	vùng mạng và phòng chống xâm nhập		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 sản phẩm phòng chống mã độc cài đặt với từng máy tính cá nhân, được giám sát qua hệ thống giám sát.

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/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

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/VNPT	+

Switch 1/ TPLink	+
Switch 2/ TPLink	+
Wifi/TPLink	+

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 để bảo vệ vùng DMZ	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/VNPT	+	+
Switch 1/ TPLink	+	+
Switch 2/ TPLink	+	+
Wifi/TPLink	+	+

5.2.2. Bảo đảm an toàn máy chủ: Hệ thống không có máy chủ

5.2.2.1. Xác thực

Yêu cầu	Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ;	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng
Máy chủ			
Hệ thống mạng LAN (*đáp ứng khi có máy chủ*)	+	+	+

5.2.2.2. Kiểm soát truy cập: Hệ thống không có máy chủ

Yêu cầu	Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa
Máy chủ	
Hệ thống mạng LAN (*đáp ứng khi có máy chủ*)	+

5.2.2.3. Nhật ký hệ thống: Hệ thống không có máy chủ

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
Máy chủ		
Hệ thống mạng LAN (*đáp ứng khi có máy chủ*)	+	+

5.2.2.4. Phòng chống xâm nhập

Yêu cầu	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ
Máy chủ		
Hệ thống mạng LAN (*đáp ứng khi có máy chủ*)	+	+

5.2.2.5. 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 cơ sở dữ liệu cho phần mềm
Máy chủ	
Hệ thống mạng LAN (*đáp ứng khi có máy chủ*)	+

5.2.3. Bảo đảm an toàn ứng dụng

5.2.3.1. 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
Ứng dụng			
Hệ thống mạng LAN (*đáp ứng khi có ứng dụng*)	+	+	+

5.2.3.2. 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
Ứng dụng		
Hệ thống mạng LAN (*đáp ứng khi có ứng dụng*)	+	+

5.2.3.3. 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.
Ứng dụng	
Hệ thống mạng LAN (*đáp ứng khi có ứng dụng*)	+

5.2.4. Bảo đảm an toàn dữ liệu

5.2.4.1. 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 (*đáp ứng khi có máy chủ và ứng dụng*)	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