|  |
| --- |
| **ỦY BAN NHÂN DÂN TỈNH VĨNH PHÚC**  **SỞ THÔNG TIN VÀ TRUYỀN THÔNG**  **HỒ SƠ ĐỀ XUẤT CẤP ĐỘ**  **HỆ THỐNG MẠNG NỘI BỘ**  **SỞ THÔNG TIN VÀ TRUYỀN THÔNG VĨNH PHÚC**  **Tỉnh Vĩnh Phúc – 2022** |

# MỤC LỤC

[MỤC LỤC 1](#_Toc118471267)

[THUẬT NGỮ, TỪ VIẾT TẮT 1](#_Toc118471268)

[DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ 1](#_Toc118471269)

[PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN 2](#_Toc118471270)

[1. Thông tin Chủ quản hệ thống thông tin 2](#_Toc118471271)

[2. Thông tin Đơn vị vận hành 2](#_Toc118471272)

[3. Mô tả phạm vi, quy mô của hệ thống 2](#_Toc118471273)

[4. Mô tả cấu trúc của hệ thống 3](#_Toc118471274)

[PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT 7](#_Toc118471275)

[1. Danh mục hệ thống thông tin và cấp độ đề xuất 7](#_Toc118471276)

[2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin 7](#_Toc118471277)

[PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN 8](#_Toc118471278)

[PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 2 10](#_Toc118471279)

[1. Thiết lập chính sách an toàn thông tin 10](#_Toc118471280)

[2. Tổ chức bảo đảm an toàn thông tin 11](#_Toc118471281)

[3. Bảo đảm nguồn nhân lực 13](#_Toc118471282)

[4. Quản lý thiết kế, xây dựng hệ thống thông tin 16](#_Toc118471283)

[5. Quản lý vận hành hệ thống thông tin 18](#_Toc118471284)

[6. Phương án Quản lý rủi ro an toàn thông tin 25](#_Toc118471285)

[7. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ 25](#_Toc118471286)

[PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÀNH PHẦN CẤP ĐỘ 2 26](#_Toc118471287)

[1. Bảo đảm an toàn mạng 26](#_Toc118471288)

[2. Bảo đảm an toàn máy chủ 29](#_Toc118471289)

[3. Bảo đảm an toàn ứng dụng 29](#_Toc118471290)

[4. Bảo đảm an toàn dữ liệu 30](#_Toc118471291)

# 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 | HSĐXCĐ | Hồ sơ đề xuất cấp độ |
| 4 | LAN | Mạng nội bộ |
| 5 | WAN | Mạng tin học diện rộng |
| 6 | ATTT | An toàn thông tin |
| 7 | HTTT | Hệ thông thông tin |
| 8 | VPN | Vitural Private Network |
| 9 | DNS | Domain Name Server |

**DANH MỤC CÁC BẢNG**

[Bảng 1. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống 5](#_Toc100926451)

[Bảng 2. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống 5](#_Toc100926452)

# DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

[Hình 1. Cấu trúc logic của hệ thống 3](#_Toc100926449)

[Hình 2. Kết nối vật lý của hệ thống 4](#_Toc100926450)

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

## **Thông tin Chủ quản hệ thống thông tin**

- Tên Tổ chức: UBND tỉnh Vĩnh Phúc

- Người đại diện: Ông Lê Duy Thành, Chức vụ: Chủ tịch UBND Tỉnh. Địa chỉ: 38 Nguyễn Trãi, Vĩnh Yên, Vĩnh Phúc.

- Thông tin liên hệ: 0211.386.1169, vpubnd@vinhphuc.gov.vn.

## Thông tin Đơn vị vận hành

- Tên Đơn vị vận hành: Trung tâm Hạ tầng thông tin - Sở Thông tin và Truyền thông

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 2942/QĐ-UBND ngày 21/10/2013 của UBND tỉnh Vĩnh Phúc về việc Thành lập Trung tâm Hạ tầng thông tin tỉnh Vĩnh Phúc; Quyết định số Quyết định số 304/QĐ-STTTT ngày 04/11/2022 về việc bảo đảm an toàn thông tin mạng trong triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông.

- Người đại diện: Ông Trần Đức Năng, Chức vụ: Giám đốc.

- Địa chỉ: Tầng 5 - Tòa nhà Sở Thông tin và Truyền thông, số 396, đường Mê Linh, Khai Quang, Vĩnh Yên, Vĩnh Phúc.

- Thông tin liên hệ: 0211.3840292.

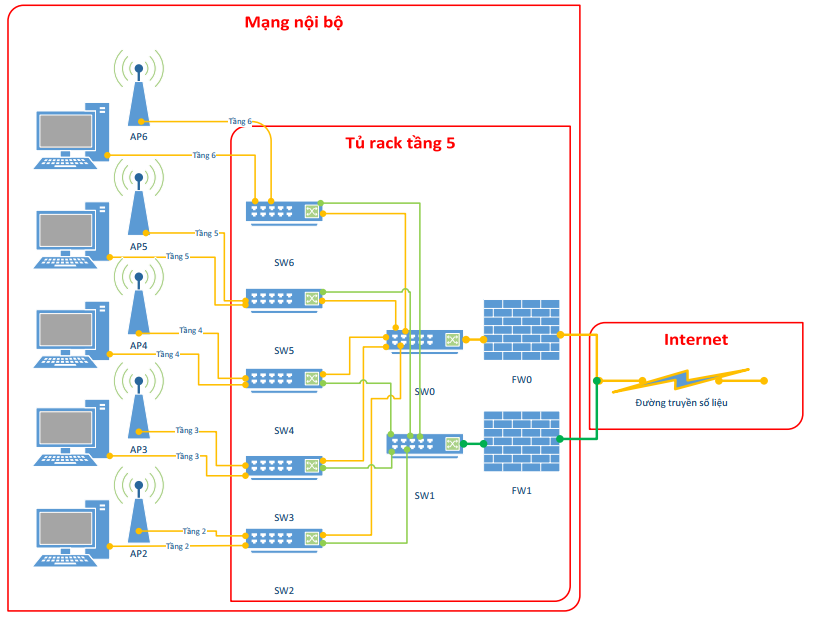
## Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô: Hệ thống mạng nội bộ Sở Thông tin và Truyền thông được thiết lập để phục vụ kết nối các máy tính trong nội bộ cơ quan và có kết nối ra Internet.

- Đối tượng phục vụ của hệ thống: Các phòng, đơn vị trực thuộc; công chức, viên chức và người lao động thuộc Sở Thông tin và Truyền thông.

## Mô tả cấu trúc của hệ thống

### Sơ đồ logic tổng thể

****

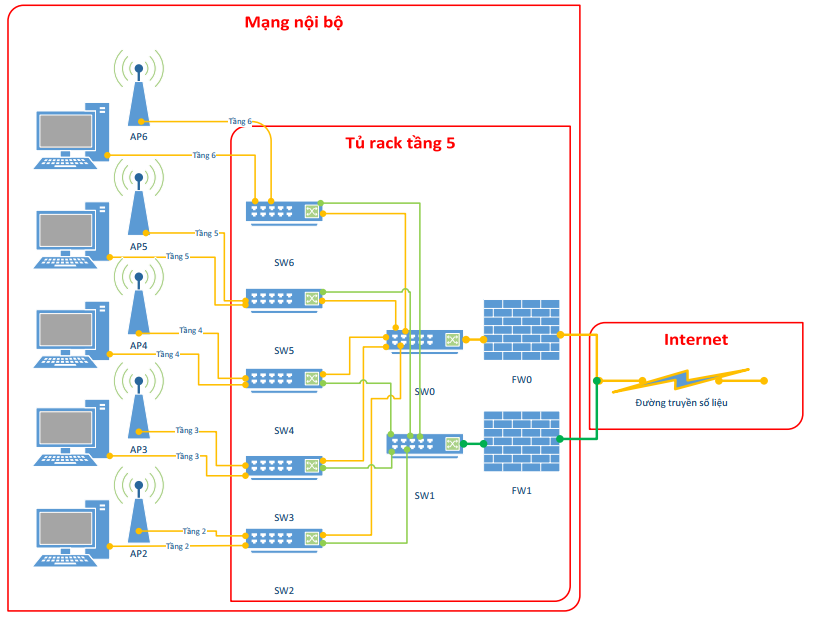
Hình 1. Cấu trúc logic của hệ thống

Các vùng mạng được thiết kế như sau:

+ Đường truyền số liệu chuyên dùng cung cấp đường truyền vào, ra Internet với hệ thống mạng nội bộ

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

### Sơ đồ kết nối vật lý

****

Hình 2. Kết nối vật lý của hệ thống

Đường truyền số liệu chuyên dùng cung cấp đường truyền vào, ra Internet với hệ thống mạng nội bộ.

Vùng mạng nội bộ đặt các thiết bị mạng, bảo mật, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống, trong đó:

Thiết bị Firewall (FW0, FW1): tường lửa bảo vệ an toàn thông tin cho kết nối mạng nội bộ vào, ra Internet.

Thiết bị WIFI lắp đặt tại các tầng sẽ kết nối các thiết bị không dây (laptop, smartphone, …) với mạng nội bộ và mạng internet.

Thiết bị Switch lắp đặt trong Tủ Rack đặt tại tầng 5, dây cáp mạng UTP sẽ kết nối các máy tính cá nhân, các thiết bị ngoại vi như máy in, máy fax, máy photo, … với hệ thống mạng nội bộ.

### Danh mục thiết bị sử dụng trong hệ thống

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên thiết bị/**  **Chủng loại** | **Vị trí triển khai** | **Mục đích sử dụng** |
| 1 | FW0/Juniper SRX 3400 | Vùng mạng nội bộ | Tường lửa bảo vệ an toàn thông tin cho kết nối mạng nội bộ vào, ra Internet |
| 2 | FW1/Juniper SRX 3400 | Vùng mạng nội bộ | Tường lửa dự phòng khi FW0/Juniper SRX 3400 gặp sự cố |
| 3 | SW0/ Juniper EX 2200 | Vùng mạng nội bộ | Nhận tín hiệu từ bộ chuyển đổi đường truyền số liệu. |
| 4 | SW1/ Juniper EX 2200 | Vùng mạng nội bộ | Switch dự phòng khi SW0/ Juniper EX 2200 gặp sự cố |
| 5 | SW2/ Juniper EX 2200 | Vùng mạng nội bộ | Kết nối với người dùng ở tầng 2 tòa nhà. |
| 6 | SW3/ Juniper EX 2200 | Vùng mạng nội bộ | Kết nối với người dùng ở tầng 3 tòa nhà. |
| 7 | SW4/ Juniper EX 2200 | Vùng mạng nội bộ | Kết nối với người dùng ở tầng 4 tòa nhà. |
| 8 | SW5/ Juniper EX 2200 | Vùng mạng nội bộ | Kết nối với người dùng ở tầng 5 tòa nhà. |
| 9 | SW6/ Juniper EX 2200 | Vùng mạng nội bộ | Kết nối với người dùng ở tầng 6 tòa nhà. |
| 10 | AP2 | Vùng mạng nội bộ | Bộ phát sóng Wifi kết nối Internet các thiết bị tầng 2 |
| 11 | AP3 | Vùng mạng nội bộ | Bộ phát sóng Wifi kết nối Internet các thiết bị tầng 3 |
| 12 | AP4 | Vùng mạng nội bộ | Bộ phát sóng Wifi kết nối Internet các thiết bị tầng 4 |
| 13 | AP5 | Vùng mạng nội bộ | Bộ phát sóng Wifi kết nối Internet các thiết bị tầng 5 |
| 14 | AP6 | Vùng mạng nội bộ | Bộ phát sóng Wifi kết nối Internet các thiết bị tầng 6 |

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

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

Hệ thống mạng nội bộ Sở Thông tin và Truyền thông là hệ thống cơ sở hạ tầng kết nối các máy tính, thiết bị công nghệ thông tin, không cung cấp dịch vụ ra ngoài Internet.

### Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Vùng mạng** | **IP Private** | **IP Public** |
| 1 | Vùng mạng nội bộ | 10.140.15.0/24 | 14.238.3.231/32 |

# PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

## Danh mục hệ thống thông tin và cấp độ đề xuất

Hệ thống mạng nội bộ Sở Thông tin và Truyền thông bao gồm hệ thống thành phần với cấp độ đề xuất tương ứng, bao gồm:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hệ thống** | **Cấp độ đề xuất** | **Căn cứ đề xuất** |
| 1 | Hệ thống mạng nội bộ Sở Thông tin và Truyền thông | 2 | Khoản 3, Điều 8, Nghị định 85/2016/NĐ-CP |

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

Hệ thống mạng nội bộ Sở Thông tin và Truyền thông chỉ xử lý thông tin công khai và phục vụ hoạt động nội bộ cho cán bộ của Sở. 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

**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

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

7. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

**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 08 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống mạng nội bộ Sở Thông tin và Truyền thông sẽ bao gồm các thuyết minh thành phần sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hệ thống** | **Cấp độ đề xuất** | **Nội dung thuyết minh** |
| 1 | Thuyết minh phương án đáp ứng yêu cầu quản lý | 2 | Phụ lục I |
| 2 | Thuyết minh phương án đáp ứng yêu cầu kỹ thuật | 2 | Phụ lục II |

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

## Thiết lập chính sách an toàn thông tin

### Chính sách an toàn thông tin

|  |  |
| --- | --- |
| **Yêu cầu** | Xây dựng chính sách an toàn thông tin. |
| **Hiện trạng** | Sở Thông tin và Truyền thông đã ban hành Quyết định số 304/QĐ-STTTT ngày 4/11/2022 về việc bảo đảm an toàn thông tin mạng trong triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông. Theo đó, Quy định đã có các chính sách về bảo đảm an toàn mạng và quản lý an toàn người sử dụng đầu cuối. |
| **Phương án** | 1. **Quản lý an toàn mạng:**   Quy định tại Điều 9, Quyết định số 304/QĐ-STTTT ngày 4/11/2022.   1. **Quản lý an toàn máy chủ và ứng dụng:**   *(Hệ thống mạng nội bộ không có máy chủ và ứng dụng).*   1. **Quản lý an toàn dữ liệu:**   Quy định tại Điều 11, Quyết định số 304/QĐ-STTTT ngày 4/11/2022.   1. **Quản lý an toàn người sử dụng đầu cuối:**   Quy định tại Điều 9; Điều 12, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |

### Xây dựng và công bố

|  |  |
| --- | --- |
| **Yêu cầu** | Quy định về xây dựng và công bố Quy chế bảo đảm an toàn thông tin. |
| **Hiện trạng** | Sở Thông tin và Truyền thông đã ban hành Quyết định số 304/QĐ-STTTT ngày 4/11/2022 về việc bảo đảm an toàn thông tin mạng trong triển khai các nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông.  Việc sửa đổi bổ sung được quy định tại Điều 21, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Xây dựng và công bố Quy định bảo đảm an toàn thông tin  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:  1. Quy chế được lấy ý kiến cấp có thẩm quyền, đơn vị liên quan trước khi công bố áp dụng.  2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Bộ phận chuyên trách để xem xét, bổ sung, sửa đổi. |

### Rà soát, sửa đổi

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin. |
| **Hiện trạng** | Việc sửa đổi bổ sung được quy định tại Khoản 6, Điều 17 và Điều 21, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin:  1. Định kỳ 03 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.  2. Trong quá trình thực hiện, nếu phát sinh các vấn đề vướng mắc hoặc cần sửa đổi, bổ sung, các phòng, đơn vị kịp thời phản ánh về Trung tâm Hạ tầng thông tin để tổng hợp, báo cáo Lãnh đạo Sở xem xét, điều chỉnh, bổ sung cho phù hợp. |

## Tổ chức bảo đảm an toàn thông tin

### 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. |
| **Hiện trạng** | Bộ phận chuyên trách về an toàn thông tin được chỉ định tại Điều 5, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Giao Trung tâm Hạ tầng thông tin là Đơn vị chịu trách nhiệm vận hành hệ thống mạng của Tòa nhà Sở Thông tin và Truyền thông; thực thi, triển khai các biện pháp bảo đảm an toàn thông tin trong cho các hệ thống thông tin của Sở Thông tin và Truyền thông; Là đầu mối của Sở Thông tin và Truyền thông trong tiếp nhận, hỗ trợ, hướng dẫn; phối hợp xử lý, điều phối ứng cứu sự cố an toàn thông tin mạng. |

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

#### 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** | Bộ phận chuyên trách về an toàn thông tin được chỉ định tại Khoản 2, Điều 5, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:  Giao Trung tâm Hạ tầng thông tin là Đơn vị chịu trách nhiệm vận hành hệ thống mạng của Tòa nhà Sở Thông tin và Truyền thông; thực thi, triển khai các biện pháp bảo đảm an toàn thông tin trong cho các hệ thống thông tin của Sở Thông tin và Truyền thông; Là đầu mối của Sở Thông tin và Truyền thông trong tiếp nhận, hỗ trợ, hướng dẫn; phối hợp xử lý, điều phối ứng cứu sự cố an toàn thông tin mạng. |

#### 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** | Bộ phận chuyên trách về an toàn thông tin được chỉ định tại Khoản 2, Điều 5, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:  Giao Trung tâm Hạ tầng thông tin là Đơn vị chịu trách nhiệm vận hành hệ thống mạng của Tòa nhà Sở Thông tin và Truyền thông; thực thi, triển khai các biện pháp bảo đảm an toàn thông tin trong cho các hệ thống thông tin của Sở Thông tin và Truyền thông; Là đầu mối của Sở Thông tin và Truyền thông trong tiếp nhận, hỗ trợ, hướng dẫn; phối hợp xử lý, điều phối ứng cứu sự cố an toàn thông tin mạng. |

#### 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** | Bộ phận chuyên trách về an toàn thông tin được chỉ định tại Khoản 2, Điều 5, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:  Giao Trung tâm Hạ tầng thông tin là Đơn vị chịu trách nhiệm vận hành hệ thống mạng của Tòa nhà Sở Thông tin và Truyền thông; thực thi, triển khai các biện pháp bảo đảm an toàn thông tin trong cho các hệ thống thông tin của Sở Thông tin và Truyền thông; Là đầu mối của Sở Thông tin và Truyền thông trong tiếp nhận, hỗ trợ, hướng dẫn; phối hợp xử lý, điều phối ứng cứu sự cố an toàn thông tin mạng. |

## Bảo đảm nguồn nhân lực

### Tuyển dụng

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ |
| **Hiện trạng** | Quy định tại Điều 6, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ:  Công chức, viên chức, người lao động tuyển dụng hoặc sắp xếp, giao nhiệm vụ về an toàn thông tin có trình độ, chuyên ngành phù hợp yêu cầu đối với các vị trí việc làm về công nghệ thông tin, an toàn thông tin theo hướng dẫn của Bộ Thông tin và Truyền thông. |

### Trong quá trình làm việc

#### 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** | Được quy định tại Điều 17, Điều 19, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc:  **Trách nhiệm của Trung tâm Hạ tầng thông tin**  1. Chủ trì phối hợp với phòng Công nghệ thông tin triển khai quy định này.  2. Tham mưu, đề xuất với Lãnh đạo Sở biện pháp quản lý, vận hành; nâng cấp hệ thống mạng nội bộ và triển khai các biện pháp bảo đảm an toàn thông tin đáp ứng nhiệm vụ chuyển đổi số phục vụ hoạt động của Sở Thông tin và Truyền thông.  3. Giám sát, nhắc nhở công chức, viên chức, người lao động thay đổi mật khẩu thường xuyên.  4. Hướng dẫn, hỗ trợ, khuyến cáo các rủi ro do mã độc gây ra cho công chức, viên chức, người lao động trong toàn cơ quan.  5. Thường xuyên cập nhật các quy định mới về bảo đảm an toàn thông tin mạng trong quá trình vận hành hệ thống; đề xuất phương án bảo đảm an toàn thông tin cho hệ thống mạng và các hệ thống thông tin khi có thay đổi về thiết kế.  6. Định kỳ 03 năm hoặc khi có thay đổi chính sách an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.  7. Cung cấp thông tin, dữ liệu phục vụ thanh tra, kiểm tra, giải quyết khiếu nại, tố cáo về bảo đảm an toàn thông tin khi cấp có thẩm quyền yêu cầu.  **Trách nhiệm của công chức và người lao động trong cơ quan**  1. Nghiêm túc chấp hành quy định này và các quy định khác của pháp luật về an toàn thông tin. Chịu trách nhiệm bảo đảm an toàn thông tin trong phạm vi trách nhiệm và quyền hạn được giao.  2. Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin phải báo cáo ngay với cấp trên và Trung tâm Hạ tầng thông tin để kịp thời ngăn chặn và xử lý.  3. Tham gia đầy đủ các chương trình diễn tập, tập huấn về an toàn thông tin mạng do Sở Thông tin và Truyền thông, Bộ Thông tin và Truyền thông tổ chức. |

#### 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** | Được quy định tại Điểm b, Khoản 2, Điều 6, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | - Tổ chức, nâng cao nhận thức về an toàn thông tin được lồng ghép vào các buổi học Nghị quyết, sinh hoạt chi bộ.  - Cử cán bộ chuyên trách tham gia các chương trình diễn tập, tập huấn về an toàn thông tin do các cơ quan chức năng tổ chức.  - Các thông tin tuyên truyền, phổ biến kiến thức về an toàn thông tin phải được phổ biến đến 100% công chức, viên chức và người lao động trong cơ quan trên Phần mềm Quản lý văn bản và Điều hành. |

### Chấm dứt hoặc thay đổi công việc

#### 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.

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc |
| **Hiện trạng** | Được quy định tại Khoản 3, Điều 6, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Chấm dứt hoặc thay đổi công việc  a) Công chức, viên chức, người lao động nghỉ việc hoặc thay đổi công việc phải thu hồi các tài khoản, quyền truy cập hệ thống, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của cơ quan.  b) Văn phòng Sở, Trưởng các phòng, Giám đốc các đơn vị trực thuộc có trách nhiệm phối hợp với Trung tâm Hạ tầng thông tin trong việc thù hồi tài sản, tài khoản, quyền truy cập của công chức, viên chức và người lao động nghỉ việc. |

#### **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.**

|  |  |
| --- | --- |
| **Yêu cầu** | 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** | Được quy định tại Điểm b, Khoản 3, Điều 6, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | 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. |

## Quản lý thiết kế, xây dựng hệ thống thông tin

### Thiết kế an toàn hệ thống thông tin

#### 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** | Được quy định tại Khoản 1, Điều 7, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Tham mưu Lãnh đạo Sở phê duyệt tài liệu mô tả về hệ thống mạng nội bộ.  Yêu cầu phải có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin |
| **Hiện trạng** | Được quy định tại Khoản 1, Điều 7, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Tham mưu Lãnh đạo Sở phê duyệt tài liệu mô tả về hệ thống mạng nội bộ. |

#### 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 |
| **Phương án** | Phương án bảo đảm an toàn thông tin theo cấp độ được mô tả tại Phụ lục II tài liệu này. |

#### 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** | Được quy định tại Khoản 1, Điều 7, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Tham mưu Lãnh đạo Sở phê duyệt tài liệu mô tả về phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin cho hệ thống mạng nội bộ. |

#### 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** | Được quy định tại các Khoản 2, Điều 7, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Thiết kế an toàn hệ thống thông tin  Khi hệ thống thông tin có thay đổi thiết kế cần đánh giá lại tính phù hợp của phương án bảo đảm an toàn thông tin để kịp thời sửa đổi, bổ sung. |

### Phát triển phần mềm thuê khoán

*(Hệ thống mạng nội bộ không bao gồm phần mềm nên không thuyết minh yêu cầu này)*

## Quản lý vận hành hệ thống thông tin

### Quản lý an toàn mạng

#### 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** | Được quy định tại Điều 9, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | 1. Công chức, viên chức và người lao động trong cơ quan khi sử dụng máy tính trong mạng nội bộ không được tự ý thay đổi địa chỉ IP và địa chỉ Default gateway đã được cấp mặc định.  2. Không được tự ý lắp đặt các thiết bị thu, phát sóng Wifi (Access Point, Router Wifi) vào mạng khi chưa thống nhất với Đơn vị vận hành mạng nội bộ.  3. Thiết bị mạng không dây trong mạng nội bộ phải được đặt mật khẩu truy cập, thường xuyên thay đổi; sao lưu các tập tin cấu hình hệ thống của các thiết bị quan trọng để sẵn sàng khôi phục khi xảy ra sự cố.  4. Không cung cấp mật khẩu của các thiết bị phát sóng Wifi trong mạng nội bộ ra bên ngoài, trừ các đoàn công tác đến làm việc trực tiếp với đơn vị.  5. Việc sử dụng mạng riêng ảo (VPN - Virtual Private Network) khi có nhu cầu làm việc từ xa, bắt buộc phải đặt mật khẩu với độ an toàn cao theo quy định tại Khoản 7, Điều 10 và thay đổi mật khẩu tối thiểu 03 lần/tháng.  6. Hạn chế tối đa sử dụng chức năng chia sẻ tài nguyên trên các máy tính cá nhân (sharing), trừ máy in. Trường hợp cần thiết sử dụng chức năng này, bắt buộc phải thiết lập mật khẩu và thực hiện việc thu hồi chức năng này khi đã sử dụng xong. |

#### 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** | Được quy định tại Khoản 3, Điều 9, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:  Thiết bị mạng không dây trong mạng nội bộ phải được đặt mật khẩu truy cập, thường xuyên thay đổi; sao lưu các tập tin cấu hình hệ thống của các thiết bị quan trọng để sẵn sàng khôi phục khi xảy ra sự cố. |

#### Truy cập và quản lý cấu hình hệ thống

|  |  |
| --- | --- |
| **Yêu cầu** | Truy cập và quản lý cấu hình hệ thống |
| **Hiện trạng** | Được quy định tại Khoản 3, Điều 10, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Thiết bị mạng không dây trong mạng nội bộ phải được đặt mật khẩu truy cập, thường xuyên thay đổi; sao lưu các tập tin cấu hình hệ thống của các thiết bị quan trọng để sẵn sàng khôi phục khi xảy ra sự cố. |

### Quản lý an toàn máy chủ và ứng dụng

*(Hệ thống mạng nội bộ không bao gồm phần máy chủ và ứng dụng nên không thuyết minh yêu cầu này)*

### Quản lý an toàn dữ liệu

#### 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** | Được quy định tại Điều 11, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | 1. Các phòng, đơn vị được giao chủ trì quản lý, sử dụng hệ thống thông tin nào có trách nhiệm tự sao lưu dữ liệu cá nhân phục vụ công tác chuyên môn.  2. Với các dữ liệu của hệ thống thông tin nghiệp vụ dùng chung trong toàn cơ quan, Trung tâm Hạ tầng thông tin có trách nhiệm sao lưu dự phòng vào thiết bị lưu trữ chuyên dụng.  3. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các dữ liệu quan trọng khác trên hệ thống (nếu có). |

#### 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** | Được quy định tại Khoản 3, Điều 11, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các dữ liệu quan trọng khác trên hệ thống (nếu có). |

### Quản lý sự cố an toàn thông tin

#### Phân nhóm sự cố an toàn thông tin mạng

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về phân nhóm sự cố an toàn thông tin mạng |
| **Hiện trạng** | Được quy định tại Khoản 1, Điều 13, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | 1. Phân loại mức độ nghiêm trọng của các sự cố, bao gồm:  a) Thấp: Sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của các phòng, đơn vị thuộc Sở Thông tin và Truyền thông.  b) Trung bình: Sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoán hay đình trệ hoạt động chính của các phòng, đơn vị thuộc Sở Thông tin và Truyền thông.  c) Cao: Sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của các phòng, đơn vị thuộc Sở Thông tin và Truyền thông.  d) Nghiêm trọng: Sự cố ảnh hưởng liên tục đến nhiều hoạt động chính của các phòng, đơn vị thuộc Sở Thông tin và Truyền thông. |

#### Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng

|  |  |
| --- | --- |
| **Yêu cầu** | Có phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng |
| **Hiện trạng** | Được quy định tại Khoản 2, Điều 13, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | 2. Xử lý sự cố:  a) Khi có sự cố tại Điểm a, b, Khoản 1 Điều này, công chức, viên chức, người lao động có trách nhiệm báo với Đơn vị vận hành mạng nội bộ để để kịp thời xử lý.  b) Khi có sự cố tại Điểm c, Khoản 1 Điều này, công chức, viên chức, người lao động có trách nhiệm báo với Đơn vị vận hành mạng nội bộ và Giám đốc Sở để xin ý kiến chỉ đạo xử lý kịp thời.  c) Đối với sự cố quy định tại Điểm d, Khoản 1 Điều này, Đơn vị vận hành mạng nội bộ báo cáo Giám đốc Sở và triển khai quy trình ứng cứu theo Quy định tại Điều 12, Quyết định số 31/2018/QĐ-UBND ngày 17/12/2018 của UBND tỉnh Vĩnh Phúc ban hành Quy định bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước tỉnh Vĩnh Phúc. |

#### Kế hoạch ứng phó sự cố an toàn thông tin mạng

|  |  |
| --- | --- |
| **Yêu cầu** | Xây dựng kế hoạch ứng phó sự cố an toàn thông tin mạng |
| **Hiện trạng** | Được quy định tại Khoản 3, Điều 13, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Trung tâm Hạ tầng thông tin có trách nhiệm tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý giám sát, phát hiện và cảnh báo sự cố an toàn thông tin |
| **Hiện trạng** | Được quy định tại Khoản 3, Điều 13, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Trung tâm Hạ tầng thông tin có trách nhiệm tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy trình ứng cứu sự cố an toàn thông tin mạng thông thường |
| **Hiện trạng** | Được quy định tại Khoản 3, Điều 13, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Trung tâm Hạ tầng thông tin có trách nhiệm tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin. |

#### Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng |
| **Hiện trạng** | Được quy định tại Khoản 3, Điều 13, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Trung tâm Hạ tầng thông tin có trách nhiệm tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin. |

#### Cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin |
| **Hiện trạng** | Được quy định tại Khoản 3, Điều 13, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Trung tâm Hạ tầng thông tin có trách nhiệm tham mưu chính sách, quy trình quản lý sự cố an toàn thông tin. |

### Quản lý an toàn người sử dụng đầu cuối

#### Quản lý truy cập, sử dụng tài nguyên nội bộ

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý truy cập, sử dụng tài nguyên nội bộ |
| **Hiện trạng** | Được quy định tại Điều 12, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | 1. Không cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn trên máy tính của cơ quan.  2. Máy trạm phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 15 phút không sử dụng. Trường hợp không sử dụng trong thời gian quá 02 giờ trở lên phải tắt máy để bảo đảm an toàn.  3. Mỗi công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và thường xuyên thay đổi để tăng cường công tác bảo mật.  4. Công chức, viên chức và người lao động có trách nhiệm triển khai các biện pháp phòng chống mã độc theo hướng dẫn của Đơn vị vận hành mạng nội bộ.  5. Không tự ý gỡ bỏ các phần mềm phòng chống mã độc trên máy tính. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật. Tất cả các tập tin, thư mục khi sao chép vào máy tính từ thiết bị ngoại vi phải được quét mã độc trước khi thực hiện.  6. Không truy cập vào các hệ thống thông tin công cộng không rõ về nội dung hoặc có nội dung phản cảm, không phù hợp với thuần phong mỹ tục của Việt Nam. Không đọc thư điện tử hoặc tải tệp tin đính kèm trong thư không rõ người gửi; Không kích hoạt các đường liên kết có dấu hiệu không rõ ràng. |

#### Quản lý truy cập mạng và tài nguyên trên Internet

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý truy cập mạng và tài nguyên trên Internet |
| **Hiện trạng** | Được quy định tại Điều 12, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | 1. Không cài đặt các phần mềm không rõ nguồn gốc, không liên quan đến công việc chuyên môn trên máy tính của cơ quan.  2. Máy trạm phải được đặt mật khẩu truy cập và thiết lập chế độ tự động bảo vệ màn hình sau 15 phút không sử dụng. Trường hợp không sử dụng trong thời gian quá 02 giờ trở lên phải tắt máy để bảo đảm an toàn.  3. Mỗi công chức, viên chức và người lao động phải tự đặt mật khẩu đăng nhập vào các hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự, có ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt như !, @, #, $, %,...) và thường xuyên thay đổi để tăng cường công tác bảo mật.  4. Công chức, viên chức và người lao động có trách nhiệm triển khai các biện pháp phòng chống mã độc theo hướng dẫn của Đơn vị vận hành mạng nội bộ.  5. Không tự ý gỡ bỏ các phần mềm phòng chống mã độc trên máy tính. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật. Tất cả các tập tin, thư mục khi sao chép vào máy tính từ thiết bị ngoại vi phải được quét mã độc trước khi thực hiện.  6. Không truy cập vào các hệ thống thông tin công cộng không rõ về nội dung hoặc có nội dung phản cảm, không phù hợp với thuần phong mỹ tục của Việt Nam. Không đọc thư điện tử hoặc tải tệp tin đính kèm trong thư không rõ người gửi; Không kích hoạt các đường liên kết có dấu hiệu không rõ ràng. |

## Phương án Quản lý rủi ro an toàn thông tin

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý truy cập mạng và tài nguyên trên Internet |
| **Hiện trạng** | Được quy định tại Điều 14, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | 1. Nội dung kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin  a) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.  b) Đánh giá hiệu quả của biện pháp bảo đảm an toàn hệ thống thông tin.  c) Đánh giá phát hiện mã độc, lỗ hổng hệ thống.  d) Kiểm tra, đánh giá khác do chủ quản hệ thống thông tin quy định.  2. Hình thức kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin  a) Định kỳ theo kế hoạch của chủ quản hệ thống thông tin.  b) Kiểm tra, đánh giá đột xuất theo yêu cầu của cấp có thẩm quyền. |

## Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý truy cập mạng và tài nguyên trên Internet |
| **Hiện trạng** | Được quy định tại Điều 15, Quyết định số 304/QĐ-STTTT ngày 4/11/2022. |
| **Phương án** | Hệ thống thông tin khi kết thúc vận hành, khai thác hoặc thanh lý, hủy bỏ phải tuân thủ các quy định của Pháp luật về quản lý tài sản. Thông tin, dữ liệu trên các hệ thống thông tin phải được sao lưu và chuyển sang các hệ thống khác (nếu còn giá trị sử dụng). Thực hiện các biện pháp xóa, hủy dữ liệu trước khi thanh lý, thanh hủy tài sản. |

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

Hệ thống mạng nội bộ Sở thông tin và Truyền thông được đề xuất là cấp độ 2. Do đó, các thành phần trong hệ thống được thuyết minh phương án đáp ứng yêu cầu cấp độ 2 như sau:

## Bảo đảm an toàn mạng

### 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 | Hệ thống mạng nội bộ cho người dùng |
| 2 | Vùng mạng biên | Có | Hệ thống kết nối với mạng truyền số liệu, được vận hành bởi Trung tâm Hạ tầng thông tin. |

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 | NA | Hệ thống không cung cấp dịch vụ truy cập từ xa |
| 2 | Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập | NA | Chỉ sử dụng vùng mạng nội bộ |
| 3 | Phương án dự phòng cho các thiết bị mạng chính | Có |  |

### Kiểm soát truy cập từ bên ngoài mạng

Hệ thống mạng nội bộ Sở Thông tin và Truyền thông chỉ phục vụ nội bộ, không cho phép truy cập từ bên ngoài.

### 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 | 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 Mạng truyền số liệu được vận hành bởi Trung tâm Hạ tầng thông tin. |

### Nhật ký hệ thống

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống | Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian |
| **Thiết bị** |
| FW0/Juniper SRX 3400 | + | + |
| FW1/Juniper SRX 3400 | + | + |
| SW0/ Juniper EX 2200 | + | + |
| SW1/ Juniper EX 2200 | + | + |
| SW2/ Juniper EX 2200 | + | + |
| SW3/ Juniper EX 2200 | + | + |
| SW4/ Juniper EX 2200 | + | + |
| SW5/ Juniper EX 2200 | + | + |
| SW6/ Juniper EX 2200 | + | + |
| AP2 | + | + |
| AP3 | + | + |
| AP4 | + | + |
| AP5 | + | + |
| AP6 | + | + |

### Phòng chống xâm nhập

Hệ thống mạng nội bộ Sở Thông tin và Truyền thông chỉ phục vụ nội bộ, không cung cấp dịch vụ ra bên ngoài Internet.

### 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** |
| FW0/Juniper SRX 3400 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| FW1/Juniper SRX 3400 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| SW0/ Juniper EX 2200 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| SW1/ Juniper EX 2200 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| SW2/ Juniper EX 2200 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| SW3/ Juniper EX 2200 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| SW4/ Juniper EX 2200 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| SW5/ Juniper EX 2200 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| SW6/ Juniper EX 2200 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| AP2 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| AP3 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| AP4 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| AP5 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |
| AP6 | + | Chỉ cho phép truy cập nội bộ | Chỉ cho phép truy cập nội bộ |

## Bảo đảm an toàn máy chủ

Hệ thống mạng nội bộ Sở Thông tin và Truyền thông không có máy chủ.

## Bảo đảm an toàn ứng dụng

Hệ thống mạng nội bộ Sở Thông tin và Truyền thông không cung cấp dịch vụ, ứng dụng.

## Bảo đảm an toàn dữ liệu

### 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 được lưu trữ mã hóa sử dụng EAS 256 |

### 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 | Có 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 trên ổ cứng di động |