|  |
| --- |
| **ỦY BAN NHÂN DÂN TỈNH ĐỒNG NAI**  **SỞ CÔNG THƯƠNG**  **HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 2 CHO HỆ THỐNG CƠ SỞ HẠ TẦNG THÔNG TIN NỘI BỘ**  **CỦA SỞ CÔNG THƯƠNG**  **ĐỒNG NAI - 2023** |

# MỤC LỤC

[MỤC LỤC 1](#_Toc116482114)

[THUẬT NGỮ, TỪ VIẾT TẮT 1](#_Toc116482115)

[DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ 3](#_Toc116482116)

[PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN 4](#_Toc116482117)

[1. Thông tin Chủ quản hệ thống thông tin 4](#_Toc116482118)

[2. Thông tin Đơn vị vận hành 4](#_Toc116482119)

[3. Mô tả phạm vi, quy mô của hệ thống 4](#_Toc116482120)

[4. Mô tả cấu trúc của hệ thống 5](#_Toc116482121)

[PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT 9](#_Toc116482122)

[1. Danh mục hệ thống thông tin và cấp độ đề xuất 9](#_Toc116482123)

[2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin 9](#_Toc116482124)

[PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN 10](#_Toc116482125)

[PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 2 12](#_Toc116482126)

[6.1.1. Thiết lập chính sách an toàn thông tin 12](#_Toc116482127)

[6.1.2. Tổ chức bảo đảm an toàn thông tin 14](#_Toc116482128)

[6.1.3. Bảo đảm nguồn nhân lực 16](#_Toc116482129)

[6.1.4. Quản lý thiết kế, xây dựng hệ thống thông tin 18](#_Toc116482130)

[6.1.5. Quản lý vận hành hệ thống thông tin 22](#_Toc116482131)

[PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÀNH PHẦN CẤP ĐỘ 2 33](#_Toc116482132)

[6.2.1. Bảo đảm an toàn mạng 33](#_Toc116482133)

[6.2.2. Bảo đảm an toàn máy chủ 38](#_Toc116482134)

[6.2.3. Bảo đảm an toàn ứng dụng 40](#_Toc116482135)

[6.2.4. Bảo đảm an toàn dữ liệu 42](#_Toc116482136)

# 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 | CSTTTH | Cơ sở truyền thanh - truyền hình |
| 7 | ĐTT | Đài truyền thanh |

**DANH MỤC CÁC BẢNG**

[Bảng 1. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống 7](#_Toc100926451)

[Bảng 2. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống 7](#_Toc100926452)

# DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

[Hình 1. Cấu trúc logic của hệ thống 5](#_Toc100926449)

[Hình 2. Kết nối vật lý của hệ thống 6](#_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 Đồng Nai.**

* Tên Tổ chức: Ủy ban nhân dân tỉnh Đồng Nai
* Quy định chức năng, nhiệm vụ và quyền hạn: Cơ quan chủ quản hệ thống thông tin của tỉnh Đồng Nai
* Người đại diện: Võ Tấn Đức; chức vụ: Quyền Chủ tịch UBND tỉnh.

- Địa chỉ: Số 2 Nguyễn Văn Trị, Biên Hoà, Đồng Nai.

- Thông tin liên hệ: 0251.3847292, Thư điện tử:…………………………....

## Thông tin Đơn vị vận hành

Tên tổ chức: **Sở Công Thương tỉnh Đồng Nai.**

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 46/2022/QĐ-UBND ngày 18/10/2022 của UBND tỉnh Đồng Nai.

- Người đại diện: Ông Phạm Văn Cường, Chức vụ: Giám đốc.

- Địa chỉ: Số 2 Nguyễn Văn Trị, Biên Hoà, Đồng Nai.

* Thông tin liên hệ: 0251.3823.317, Thư điện tử: sct@dongnai.gov.vn

## Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống trang thông tin điện tử Sở Công Thương tỉnh Đồng Nai: Hệ thống trang thông tin điện tử Sở Công Thương tỉnh Đồng Nai được thiết lập để phục vụ công tác chỉ đạo điều hành và cung cấp dịch vụ trong phạm vi Sở Công Thương quản lý.

- Đối tượng phục vụ của hệ thống: Cán bộ, công chức, viên chức người lao động đang công tác trong lĩnh vực Công thương.

* Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi Hệ thống:

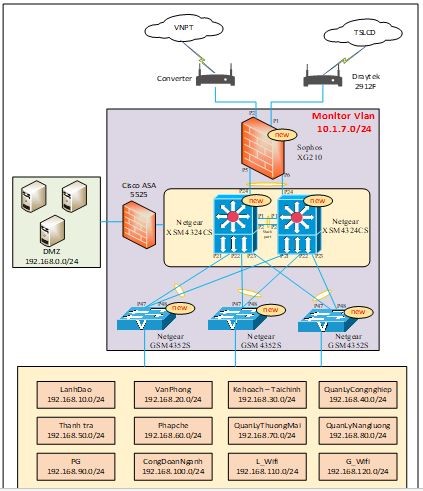
+ Hệ thống phần mềm quản lý cơ sở dữ liệu địa hình, dữ liệu quy hoạch trên địa bàn tỉnh Đồng Nai.

+ Mạng nội bộ, mạng diện rộng ngành xây dựng tỉnh Đồng Nai.

+ Hệ thống phòng cháy, chữa cháy đảm bảo hệ thống an toàn.

## Mô tả cấu trúc của hệ thống

### Mô hình logic tổng thể

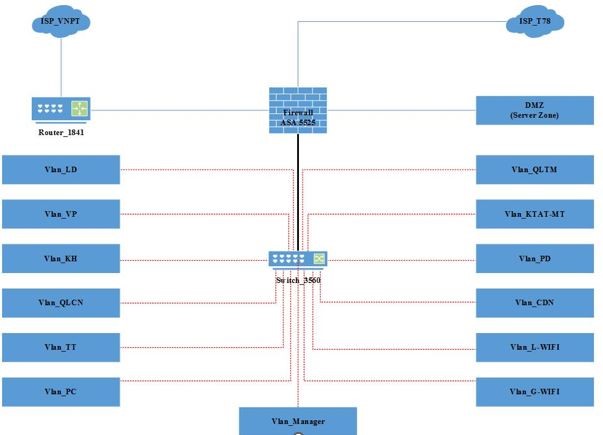
****

*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 DMZ đặt máy chủ công cộng, cung cấp dịch vụ ra bên ngoài 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.

### Mô hình kết nối vật lý

****

*Hình 2. Kết nối vật lý của hệ thống*

(Mô tả kết nối vật lý của Hệ thống)

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên thiết bị/**  **Chủng loại** | **Vị trí triển khai** | **Mục đích sử dụng** |
| 1 | Modem DrayTek Vigor2912 (Router TSLCD - 1841); Totolink F1(wan) | Vùng mạng biên | Kết nối và định tuyến động với các Router của ISP. |
| 2 | Dell PowerEdge R720 (cài Forefront TMG) | Vùng mạng biên | Bảo vệ an ninh cho mạng nội bộ |
| 3 | Thiết bị Sophos XG 210 HW Rev. 3 Appliance | Vùng mạng biên | Bảo vệ an ninh cho mạng nội bộ |
| 4 | Thiết bị chuyển mạch NETGEAR M4300-24X XSM4324CS Stackable Managed Switch | Vùng mạng nội bộ | Kết nối mạng nội bộ |
| 5 | Thiết bị chuyển mạch NETGEAR M4300-52G GSM4352S Stackable Managed Switch | Vùng mạng nội bộ | Kết nối mạng nội bộ |

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

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

*Bảng 2. Danh mục thiết bị máy chủ sử dụng trong hệ thống*

### 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 nội bộ | Web Server (Máy Ảo)/Cài đặt Web-App/Vùng DMZ/Window Server 2012  Database Server (Máy Ảo)/ Cài đặt SQL server 2012/Vùng máy chủ nội bộ/Window Server 2012 | Quản lý, điể khiển mạng - mạng Domain Control, phân chia mạng (mỗi phòng theo 1 Vlan) , băng thông. |

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Vùng mạng** | **IP Private** | **IP Public** |
| 1 | DMZ | 192.168.1.0/24 | 1 |
| 2 | Vùng mạng nội bộ | 192.168.100.0/24 | 2 |
| 3 | Vùng mạng biên | 192.168.1.2/24 | 10.174.39.38/24 |

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

# PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hệ thống** | **Cấp độ đề xuất** | **Căn cứ đề xuất** |
| 1 | Hệ thống mạng nội bộ của Sở Công Thương | 2 | Khoản 3 Điều 8 Nghị định 85/2016/NĐ-CP (Điều 8 ) |

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

Hệ thống mạng nội bộ của Sở Công Thương được xây dựng để phục vụ hoạt động nội bộ cho cán bộ của Sở Công Thương tỉnh Đồng Nai bao gồm máy móc thiết bị, hạ tầng mạng, đường truyền. Hệ thống mạng nội bộ của Sở Công Thương là hệ thống thông tin có tiêu chí cụ thể: Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của một cơ quan, tổ chức, 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.

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 HSĐXCĐ được phê duyệt.

**II. Thuyết minh phương án về kỹ thuật bao gồm các nội dung:**

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

1.2. Kiểm soát truy cập từ bên ngoài mạng

1.3. Kiểm soát truy cập từ bên trong mạng

1.4. Nhật ký hệ thống

1.5. Phòng chống xâm nhập

1.6. Bảo vệ thiết bị hệ thống

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

2.2. Kiểm soát truy cập

2.3. Nhật ký hệ thống

2.4. Phòng chống xâm nhập

2.5. Phòng chống phần mềm độc hại

2.6. Xử lý máy chủ khi chuyển giao

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

3.2. Kiểm soát truy cập

3.3. Nhật ký hệ thống

3.4. An toàn ứng dụng và mã nguồn

4. Bảo đảm an toàn dữ liệu

4.1. Bảo mật dữ liệu

4.2. Sao lưu dự phòng

Đối với các yêu cầu kỹ thuật chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, Đơn vị vận hành sẽ triển khai nâng cấp, thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong vòng 18 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 của Sở Công Thươngsẽ 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

## 6.1.1. Thiết lập chính sách an toàn thông tin

### 6.1.1.1. Chính sách an toàn thông tin

|  |  |
| --- | --- |
| **Yêu cầu** | Xây dựng chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống nhằm bảo đảm tính sẵn sàng của hệ thống trong quá trình vận hành, khai thác. |
| **Hiện trạng** | Đơn vị đã vận hành xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 về ban hành Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương |
| **Phương án** | 1. Quản lý an toàn mạng: 2. 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. 3. 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. 4. 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. 5. Quản lý an toàn máy chủ và ứng dụng:   a) Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Các hệ thống thông tin cần có phướng án giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị.  b) Kiểm tra, giám sát các hoạt động liên quan đến các nơi lưu trữ mật khẩu và cảnh báo khi có những hành động bất thường (Ví dụ: user không có quyền nhưng cố tình truy xuất đến các file lưu mật khẩu…).   1. Quản lý an toàn dữ liệu: 2. Có cơ chế sao lưu dữ liệu dự phòng, lưu trữ dữ liệu tại nơi an toàn đồng thời thường xuyên kiểm tra để đảm bảo sẵn sàng phục hồi nhằm ngăn ngừa và hạn chế khi sự cố an toàn thông tin mạng xảy ra. Dữ liệu trên máy chủ được sao lưu thông qua hệ thống sao lưu dữ liệu. 3. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống theo yêu cầu của đơn vị vận hành. 4. Quyền truy cập phải được phân ra theo từng cấp độ tương ứng với từng nhiệm vụ của nhân viên và phải được phê duyệt từ cấp trên. 5. Quản lý an toàn người sử dụng đầu cuối: 6. 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. 7. 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. 8. 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 9. 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. 10. Đơn vị chuyên trách về an toàn thông tin thường xuyên theo dõi cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống đối với các nhân viên đã nghỉ việc.  * f) Đơn vị chuyên trách về an toàn thông tin thường xuyên theo dõi cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho máy tính người sử dụng và thực hiện quy trình trước khi đưa hệ thống vào sử dụng. |

### 6.1.1.2. 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** | Đáp ứng. Đã xây dựng, công bố Quy chế bảo đảm an toàn thông tin (Tham chiếu Điều 20 theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 về ban hành Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương) |
| **Phương án** | Xây dựng và công bố Quy chế 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. |

### 6.1.1.3. 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** | Đáp ứng. Tham chiếuĐiều 21, Điều 13 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **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. Chính sách được tổ chức/ bộ phận được ủy quyền thông qua trước khi công bố áp dụng.  2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Bộ phận chuyên trách về ATTT để tổng hợp báo cáo Bộ Thông tin và Truyền thông điều chỉnh, bổ sung. |

## 6.1.2. Tổ chức bảo đảm an toàn thông tin

### 6.1.2.1. Đơn vị chuyên trách về an toàn thông tin

|  |  |
| --- | --- |
| **Yêu cầu** | Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về an toàn thông tin trong tổ chức |
| **Hiện trạng** | Đáp ứng. Tham chiếuĐiều 18 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Giao Văn phòng Sở là bộ phận chuyên trách về ATTT cho Hệ thống mạng nội bộ của Sở Công Thương |

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

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin |
| **Hiện trạng** | Đáp ứng. Tham chiếuĐiều 5 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023*)* |
| **Phương án** | Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:  a) Văn phòng Bộ Thông tin và Truyền thông giao Phòng Truyền thanh là đầu mối liên hệ, phối hợp với Cục An toàn thông tin và các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống .... |

#### 6.1.2.2.b. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin

|  |  |
| --- | --- |
| **Yêu cầu** | Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin |
| **Hiện trạng** | Đáp ứng. Tham chiếuĐiều 13 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Văn phòng Sở làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của Hệ thống thông tin. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền |
| **Hiện trạng** | Đáp ứng. Tham chiếu Điểm b Khoản 2 Điều 6 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền |

## 6.1.3. Bảo đảm nguồn nhân lực

### 6.1.3.1. Tuyển dụng

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 1 Điều 6 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **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. |

### 6.1.3.2. Trong quá trình làm việc

#### 6.1.3.2.a. Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 2 Điều 6 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **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 cán bộ quản lý và vận hành hệ thống  a) Cán bộ chuyên trách phải thiết lập phương pháp hạn chế truy cập mạng không dây, giám sát và điều khiển truy cập không dây, tổ chức sử dụng chứng thực và mã hóa để bảo vệ truy cập không dây tới hệ thống thông tin.  b) 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.  c) Các cơ quan, địa phương và các tổ chức, cá nhân tham gia sử dụng các dịch vụ của hệ thống phải tuân thủ các quy định về bảo đảm an toàn, an ninh thông tin và chịu trách nhiệm đối với mọi hoạt động trên tài khoản truy cập của mình đã được cấp trên hệ thống. |

#### 6.1.3.2.b. Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng

|  |  |
| --- | --- |
| **Yêu cầu** | Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng |
| **Hiện trạng** | Đáp ứng. Tham chiếu Điểm b Khoản 2 Điều 6 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Kế hoạch và tổ chức định kỳ hàng năm:  Kế hoạch và định kỳ hàng năm tổ chức đào tạo về an toàn thông tin cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống. |

### 6.1.3.3. Chấm dứt hoặc thay đổi công việc

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 3 Điều 6 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:  Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chức. |

b) 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** | Đáp ứng. Tham chiếu Điểm b Khoản 3 Điều 6 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **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.  Bổ sung, xây dựng quy trình vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc tại dự thảo *Quy chế vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc* trong vòng 06 tháng kể từ khi HSĐXCĐ được phê duyệt. |

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

### 6.1.4.1. Thiết kế an toàn hệ thống thông tin

#### 6.1.4.1.a. Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin

|  |  |
| --- | --- |
| **Yêu cầu** | Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin |
| **Hiện trạng** | Đáp ứng. Tham chiếu Điều 1 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Thiết kế an toàn hệ thống thông tin  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. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 2 Điều 7 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Thiết kế an toàn hệ thống thông tin  Yêu cầu phải có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 3 Điều 7 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Thiết kế an toàn hệ thống thông tin  Yêu cầu phải có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 4 Điều 7 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Thiết kế an toàn hệ thống thông tin  Yêu cầu phải có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin. |

#### 6.1.4.1.đ. Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 5 Điều 7 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Thiết kế an toàn hệ thống thông tin  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. |

### 6.1.4.2. Phát triển phần mềm thuê khoán

#### 6.1.4.2.a. Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán

|  |  |
| --- | --- |
| **Yêu cầu** | Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 1 Điều 8 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quy định đối với việc phát triển phần mềm thuê khoán:  Yêu cầu có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 2 Điều 8 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quy định đối với việc phát triển phần mềm thuê khoán:  Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm. |

### 6.1.4.3. Thử nghiệm và nghiệm thu hệ thống

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 2 Điều 9 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quy định đối với việc thử nghiệm và nghiệm thu hệ thống:  Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc thực hiện thử nghiệm và nghiệm thu hệ thống trước khi bàn giao và đưa vào sử dụng. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có yêu cầu về nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 1 Điều 9 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quy định đối với việc thử nghiệm và nghiệm thu hệ thống:  Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống.  Bổ sung quy trình thử nghiệm và nghiệm thu hệ thống tại dự thảo *Quy chế thử nghiệm và nghiệm thu hệ thống* trong vòng 06 tháng kể từ khi HSĐXCĐ được phê duyệt. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 4 Điều 9 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quy định đối với việc thử nghiệm và nghiệm thu hệ thống:  Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống. |

## 6.1.5. Quản lý vận hành hệ thống thông tin

### 6.1.5.1. Quản lý an toàn mạng

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn mạng. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống |
| **Hiện trạng** | Đáp ứng. Tham chiếu Điều 11 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ  a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.  b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.  c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.  d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.  đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.  e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 5 Điều 10 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:  Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Truy cập và quản lý cấu hình hệ thống |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 6 Điều 10 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Truy cập và quản lý cấu hình hệ thống:  Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại Trung tâm dữ liệu theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài. |

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

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn máy chủ và ứng dụng. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

**Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:**

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ |
| **Hiện trạng** | Đáp ứng. Tham chiếu Điều 11 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ:  a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn.  b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có.  c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.  d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.  đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.  e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn. |

#### **6.1.5.2.b.** Truy cập mạng của máy chủ

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định quản lý truy cập mạng của máy chủ |
| **Hiện trạng** | Đáp ứng. Tham chiếu Điều 11 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Truy cập mạng của máy chủ:  Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định quản lý truy cập và quản trị máy chủ và ứng dụng |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 4 Điều 11 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Truy cập và quản trị máy chủ và ứng dụng:  a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.  b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành.  c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố |
| **Hiện trạng** | Đáp ứng. Tham chiếu Điều 12, Điều 13 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. |

### 6.1.5.3. Quản lý an toàn dữ liệu

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn dữ liệu. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có chính sách, quy trình dự phòng và khôi phục dữ liệu |
| **Hiện trạng** | Đáp ứng. Tham chiếu Điều 12 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Yêu cầu an toàn đối với phương pháp mã hóa  a) Đơn vị phải xây dựng và áp dụng quy định sử dụng các phương thức mã hóa thích hợp theo các chuẩn quốc gia hoặc quốc tế đã được công nhận để bảo vệ thông tin.  b) Phải có biện pháp quản lý khóa mã hóa thích hợp để hỗ trợ việc sử dụng các kỹ thuật mã hóa.  2. Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.  3. Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu.  4. Sao lưu dự phòng và khôi phục dữ liệu (tần suất sao lưu dự phòng, phương tiện lưu trữ, thời gian lưu trữ; nơi lưu trữ, phương thức lưu trữ và phương thức lấy dữ liệu ra khỏi phương tiện lưu trữ. |

#### 6.1.5.3.b. Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ |
| **Hiện trạng** | Đáp ứng. Tham chiếu Khoản 2 Điều 12 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Bổ sung  Định kỳ 3 năm 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. Bản sao lưu được lưu trữ tối thiểu thành 02 bản và được lưu trữ ở hai địa chỉ khác nhau. |

### 6.1.5.4. Quản lý sự cố an toàn thông tin

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý sự cố an toàn thông tin. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

#### 6.1.5.4.a. 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** | Đáp ứng. Tham chiếu Khoản 2 Điều 12 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg 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 (Quyết định 05); 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. |

#### 6.1.5.4.b. 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** | Đáp ứng một phần. Tham chiếu Điều 13 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg. |

#### 6.1.5.4.c. 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** | Đáp ứng một phần. Tham chiếu Khoản 1 Điều 13 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/QĐ-TTg. |

#### 6.1.5.4.d. 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** | Đáp ứng một phần. Tham chiếu Khoản 4 Điều 13 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Có phương án và điều động nhân lực có kinh nghiệm thực hiện giám sát, phát hiện và cảnh báo sự cố an toàn thông tin, phối hợp với các đơn vị chuyên trách về ATTT đưa ra cảnh bảo sớm về nguy cơ mất ATTT trong hệ thống.  Đối với 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. |

#### 6.1.5.4.đ. 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** | Đáp ứng một phần. Tham chiếu Khoản 3 Điều 13 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg. |

#### 6.1.5.4.e. 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** | Đáp ứng một phần. Tham chiếu Khoản 3 Điều 13 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13, 14 Quyết định số 05/2017/QĐ-TTg. |

#### 6.1.5.4.g. 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** | Đáp ứng một phần. Tham chiếu Khoản 5 Điều 13 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | 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 |

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

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn người sử dụng đầu cuối. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

#### 6.1.5.5.a. 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** | Đáp ứng. Tham chiếu Điều 14, Điều 19 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quản lý truy cập, sử dụng tài nguyên nội bộ:  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.  c) Máy tính/thiết bị đầu cuối phải được xử lý điểm yếu an toàn thông tin, cấu hình cứng hóa bảo mật trước khi kết nối vào hệ thống. |

#### 6.1.5.5.b. 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** | Đáp ứng một phần. Tham chiếu Điều 6, Điều 13, Điều 14 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **Phương án** | Quản lý truy cập mạng và tài nguyên trên Internet:  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. |

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

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình Quản lý rủi ro an toàn thông tin. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

|  |  |
| --- | --- |
| **Yêu cầu** | Có chính sách, quy trình quản lý quản lý rủi ro an toàn thông tin |
| **Hiện trạng** | Đáp ứng. Tham chiếu Điều 15 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **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. |

### 6.1.5.7. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

|  |  |
| --- | --- |
| **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 16 Quy chế Bảo đảm an toàn, an ninh mạng Hệ thống mạng nội bộ của Sở Công Thương theo Quyết định số 308/QĐ-SCT ngày 11/12/2023 |
| **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 THÀNH PHẦN CẤP ĐỘ 2**

Hệ thống thông tin: Mạng nội bộ của Sở Công Thương được đề xuất là cấp độ 2. Do đó, các máy chủ được sử dụng để triển khai hệ thống và các thành phần khác trong hệ thống như hạ tầng mạng, hệ thống lưu trữ…được thuyết minh phương án đáp ứng yêu cầu cấp độ 2 như sau:

**6.2.1. Bảo đảm an toàn mạng**

***6.2.1.1. Thiết kế hệ thống***

a) Các vùng mạng trong hệ thống:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Vùng mạng nội bộ | Có | Cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối, các thiết bị khác của người sử dụng vào hệ thống |
| 2 | Vùng mạng biên | Có | Kết nối hệ thống với mạng Internet và mạng diện rộng |
| 3 | Vùng DMZ | Có | Đặt máy chủ WEBAPP, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet. |
| 4 | Vùng máy chủ nội bộ | Có | Là vùng đặt máy chủ cơ sở dữ liệu. |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **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 | Sử dụng Tường lửa Generic Firewall có tích hợp chức năng VPN để quản lý truy cập, quản trị hệ thống từ xa an toàn. Tính năng VPN này được cấu hình trực tiếp trên thiết bị Generic Firewall, quản lý truy cập từ bên ngoài vào vùng mạng nội bộ , từ bên ngoài vào vùng máy chủ nội bộ, từ vùng mạng nội bộ vào vùng máy chủ nội bộ |
| 2 | Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập sử dụng tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc sản phẩm chống tấn công, xâm nhập | Có | Sử dụng Tường lửa Generic Firewall có tích hợp chức năng IPS để quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập.  Tính năng IPS được cấu hình trên Generic Firewall kiểm soát truy cập và phòng chống xâm nhập giữa các phân vùng mạng nội bộ, máy chủ nội bộ và phân vùng mạng DMZ. |
| 3 | Phương án phòng chống mã độc cho máy chủ và máy trạm | có | Sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương (Giải pháp Antivirus là Bitdefender bản quyền do Sở Thông tin và Truyền thông triển khai chung cho sở ban ngành, Sở đã hoàn thành cài đặt toàn bộ cho máy chủ và máy trạm) |
| 4 | Phương án phòng chống tấn công mạng cho ứng dụng web | có | Sử dụng sản phẩm Tường lửa ứng dụng web (WAF) được đặt tại phân vùng mạng DMZ và tưởng lửa cứng Sofos |
| 5 | Phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (đối với hệ thống thư điện tử) |  | Sở sử dụng sản phẩm Bảo đảm an toàn thông tin cho hệ thống thư điện tử đối với hệ thống Thư điện tử, đáp ứng tiêu chí quy định tại khoản 2 Điều 9 Nghị định 85/2016/NĐ-CP. Sở thụ hưởng hệ thống mail công vụ do Sổ Thông tinh và Truyền với Server mail đặt tại Datacenter tỉnh |
| 6 | Phương án dự phòng cho các thiết bị mạng chính | Có | Các thiết bị mạng chính: Router, Firewall, Switch đều có thiết bị dự phòng |

***6.2.1.2. Kiểm soát truy cập từ bên ngoài mạng***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet | Có | Hệ thống sử dụng Tường lửa Generic Firewall có tích hợp chức năng VPN 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. |
| 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 | Tường lửa Generic Firewall được thiết lập chỉ cho phép 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 |
| 3 | Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng. | Có | Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng trên Tường lửa Generic Firewall và ngắt phiên kết nối VPN khi người dùng không thao tác sử dụng trong 1 khoảng thời gian |

***6.2.1.3 Kiểm soát truy cập từ bên trong mạng***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức | Có | 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 Tường lửa Generic Firewall |

***6.2.1.4. Nhật ký hệ thống***

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống | Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian |
| **Thiết bị** |
| Router outsite/ | + | + |
| Generic Firewall/ Checkpoint 12600 | + | + |
| SWDMZ/Cisco2960 | + | + |
| SWSF/ Cisco2960 | + | + |
| SW/Cisco2960 | + | + |
| SW L2/Cisco2960 | + | + |
| WAF/WAF v2secure | + | + |

***6.2.1.5. Phòng chống xâm nhập***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống | Đáp ứng | Sử dụng Tường lửa Generic Firewall có tích hợp chức năng IPS để bảo vệ các vùng mạng trong hệ thống. Tính năng IPS được cấu hình trên Generic Firewall kiểm soát truy cập và phòng chống xâm nhập giữa các phân vùng mạng nội bộ, máy chủ nội bộ và phân vùng mạng DMZ. |
| 2 | Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng | Đáp ứng | Thực hiện định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng trên Tường lửa Generic Firewall. |

***6.2.1.6. Bảo vệ thiết bị hệ thống***

|  |  |  |  |
| --- | --- | --- | --- |
| **Yêu cầu** | Cấu hình chức năng xác thực trên các thiết bị | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa | Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa |
| **Thiết bị** |
| Router outsite/ | + | + | + |
| Generic Firewall/ Checkpoint 12600 | + | + | + |
| SWDMZ/Cisco2960 | + | + | + |
| SWSF/ Cisco2960 | + | + | + |
| SW/Cisco2960 | + | + | + |
| SWL2/Cisco2960 | + | + | + |
| WAF/WAF v2secure | + | + | + |

**6.2.2. Bảo đảm an toàn máy chủ**

***6.2.2.1. Xác thực***

|  |  |  |  |
| --- | --- | --- | --- |
| **Yêu cầu** | Thiết lập chính sách xác thực trên máy chủ | Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa | Thiết lập chính sách mật khẩu an toàn: Yêu cầu thay đổi mật khẩu mặc định; Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ |
| **Máy chủ** |
| Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/ Window Server 2019 | + | + | + |
| Database Server (máy ảo)/ Cài đặt SQL server 2019/Vùng máy chủ nội bộ/ Window Server 2019 | + | + | + |

***6.2.2.2. Kiểm soát truy cập***

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa | Thiết lập giới hạn thời gian chờ (timeout) |
| **Máy chủ** |
| Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/ Window Server 2019 | + | + |
| Database Server (máy ảo)/ Cài đặt SQL server 2019/Vùng máy chủ nội bộ/ Window Server 2019 | + | + |

***6.2.2.3. Nhật ký hệ thống***

|  |  |  |  |
| --- | --- | --- | --- |
| **Yêu cầu** | Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ | Đồng bộ thời gian giữa máy chủ với máy chủ thời gian | Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 01 tháng |
| **Máy chủ** |
| Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/ Window Server 2019 | + | + | + |
| Database Server (máy ảo)/ Cài đặt SQL server 2019/Vùng máy chủ nội bộ/ Window Server 2019 | + | + | + |

***6.2.2.4. 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 | Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng | Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng |
| **Máy chủ** |
| Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/ Window Server 2019 | + | + | + | + |
| Database Server (máy ảo)/ Cài đặt SQL server 2019/Vùng máy chủ nội bộ/ Window Server 2019 | + | + | + | + |

***6.2.2.5. Phòng chống phần mềm độc hại***

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật | Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt |
| **Máy chủ** |
| Web Server (máy ảo)/Cài đặt Web-App/Vùng DMZ/ Window Server 2019 | + | + |
| Database Server (máy ảo)/ Cài đặt SQL server 2019/Vùng máy chủ nội bộ/ Window Server 2019 | + | + |

***6.2.2.6. Xử lý máy chủ khi chuyển giao***

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

**6.2.3. Bảo đảm an toàn ứng dụng**

***6.2.3.1. Xác thực***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Yêu cầu** | Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng | Lưu trữ có mã hóa thông tin xác thực hệ thống | Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng | Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định |
| **Ứng dụng** |
| Hệ thống cơ sở dữ liệu ngành công thương tỉnh Đồng Nai (*Server đặt tại Công ty*); Hệ thống thông tin khuyến mại tỉnh Đồng Nai (*Server đặt tại Datacenter tỉnh*) | + | + | + | + |

***6.2.3.2. Kiểm soát truy cập***

|  |  |  |  |
| --- | --- | --- | --- |
| **Yêu cầu** | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa | Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng | Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa |
| **Ứng dụng** |
| Hệ thống cơ sở dữ liệu ngành công thương tỉnh Đồng Nai; Hệ thống thông tin khuyến mại tỉnh Đồng Nai | + | + | + |

***6.2.3.3. Nhật ký hệ thống***

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng. | Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng |
| **Ứng dụng** |
| Hệ thống cơ sở dữ liệu ngành công thương tỉnh Đồng Nai; Hệ thống thông tin khuyến mại tỉnh Đồng Nai | + | + |

***6.2.3.4. An toàn ứng dụng và mã nguồn***

|  |  |
| --- | --- |
| **Yêu cầu** | Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý |
| **Ứng dụng** |
| Hệ thống cơ sở dữ liệu ngành công thương tỉnh Đồng Nai; Hệ thống thông tin khuyến mại tỉnh Đồng Nai | + |

## 6.2.4. Bảo đảm an toàn dữ liệu

### *6.2.4.1 Bảo mật dữ liệu*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Lưu trữ có mã hóa các thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ | Có | Dữ liệu được nén và được lưu trữ mã hóa sử dụng EAS 256 |

### *6.2.4.2 Sao lưu dự phòng*

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ | Có | 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 |