|  |
| --- |
| **(CHỦ QUẢN HỆ THỐNG THÔNG TIN)**  **(ĐƠN VỊ VẬN HÀNH)**  **HỒ SƠ MẪU**  **HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 3 (TÊN HỆ THỐNG THÔNG TIN)**  **Tỉnh A – 20xx** |

**MỤC LỤC**

[**THUẬT NGỮ, TỪ VIẾT TẮT 1**](#_Toc116481025)

[**DANH MỤC CÁC BẢNG 2**](#_Toc116481026)

[**DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ 3**](#_Toc116481027)

[**PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN 4**](#_Toc116481028)

[**1. Thông tin Chủ quản hệ thống thông tin 4**](#_Toc116481029)

[**2. Thông tin Đơn vị vận hành 4**](#_Toc116481030)

[**3. Mô tả phạm vi, quy mô của hệ thống 4**](#_Toc116481031)

[**4. Mô tả cấu trúc của hệ thống 5**](#_Toc116481032)

[**4.1. Mô hình logic tổng thể 5**](#_Toc116481033)

[**4.2. Mô hình kết nối vật lý 6**](#_Toc116481034)

[**4.3. Danh mục thiết bị sử dụng trong hệ thống 6**](#_Toc116481035)

[**4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống 9**](#_Toc116481036)

[**4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống 9**](#_Toc116481037)

[**PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT 11**](#_Toc116481038)

[**1. Danh mục hệ thống thông tin và cấp độ đề xuất 11**](#_Toc116481039)

[**2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin 11**](#_Toc116481040)

[**PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM 12**](#_Toc116481041)

[**AN TOÀN HỆ THỐNG THÔNG TIN 12**](#_Toc116481042)

[**PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 3 15**](#_Toc116481043)

[**7.1.1. Thiết lập chính sách an toàn thông tin: 15**](#_Toc116481044)

[**7.1.1.1. Chính sách an toàn thông tin 15**](#_Toc116481045)

[**Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin 15**](#_Toc116481046)

[**Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng 16**](#_Toc116481047)

[**7.1.1.2. Xây dựng và công bố 23**](#_Toc116481048)

[**7.1.1.3. Rà soát, sửa đổi 23**](#_Toc116481049)

[**7.1.2. Tổ chức bảo đảm an toàn thông tin 24**](#_Toc116481050)

[**7.1.2.1. Đơn vị chuyên trách về an toàn thông tin 24**](#_Toc116481051)

[**7.2.2.2. Phối hợp với những cơ quan/tổ chức có thẩm quyền 25**](#_Toc116481052)

[**7.1.3. Tổ chức bảo đảm an toàn thông tin 26**](#_Toc116481053)

[**7.1.3.1. Tuyển dụng 26**](#_Toc116481054)

[**7.1.3.2. Trong quá trình làm việc 29**](#_Toc116481055)

[**7.1.3.3. Chấm dứt hoặc thay đổi công việc 30**](#_Toc116481056)

[**7.1.4. Quản lý thiết kế, xây dựng hệ thống thông tin 32**](#_Toc116481057)

[**7.1.4.1. Thiết kế an toàn hệ thống thông tin 32**](#_Toc116481058)

[**7.1.4.2. Phát triển phần mềm thuê khoán 35**](#_Toc116481059)

[**7.1.4.3. Thử nghiệm và nghiệm thu hệ thống 38**](#_Toc116481060)

[**7.1.5. Quản lý vận hành hệ thống thông tin 42**](#_Toc116481061)

[**7.1.5.1. Quản lý an toàn mạng 42**](#_Toc116481062)

[**7.1.5.2. Quản lý an toàn máy chủ và ứng dụng 44**](#_Toc116481063)

[**7.1.5.3. Quản lý an toàn dữ liệu 48**](#_Toc116481064)

[**7.1.5.4. Quản lý an toàn thiết bị đầu cuối 49**](#_Toc116481065)

[**7.1.5.5. Quản lý phòng chống phần mềm độc hại 51**](#_Toc116481066)

[**7.1.5.6. Quản lý giám sát an toàn hệ thống thông tin 54**](#_Toc116481067)

[**7.1.5.7. Quản lý điểm yếu an toàn thông tin 58**](#_Toc116481068)

[**7.1.5.8. Quản lý sự cố an toàn thông tin 61**](#_Toc116481069)

[**7.1.5.9. Quản lý an toàn người sử dụng đầu cuối 69**](#_Toc116481070)

[**7.1.5.10. Quản lý rủi ro an toàn thông tin 73**](#_Toc116481071)

[**7.1.5.11. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ. 73**](#_Toc116481072)

[**PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT CẤP ĐỘ 3 75**](#_Toc116481073)

[**1. Bảo đảm an toàn mạng 75**](#_Toc116481074)

[**2. Bảo đảm an toàn máy chủ 84**](#_Toc116481075)

[**3. Bảo đảm an toàn ứng dụng 89**](#_Toc116481076)

[**4. Bảo đảm an toàn dữ liệu 92**](#_Toc116481077)

# THUẬT NGỮ, TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **Từ viết tắt** | **Nghĩa đầy đủ** |
|  | CNTT | Công nghệ thông tin |
|  | CSDL | Cơ sở dữ liệu |
|  | DVCTT | Dịch vụ công trực tuyến |
|  | MCĐT | Một cửa điện tử |
|  | WAN | Mạng tin học diện rộng |
|  | LAN | Mạng nội bộ |
|  | TSLCD | Mạng Truyền số liệu chuyên dùng |
|  | VPN | Vitural Private Network |
|  | DNS | Domain Name Server |

**DANH MỤC CÁC BẢNG**

[Bảng 1. Danh mục thiết bị sử dụng trong hệ thống 8](#_Toc116484029)

[Bảng 2. Danh mục thiết bị máy chủ sử dụng trong hệ thống 8](#_Toc116484030)

[Bảng 3. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống 9](#_Toc116484031)

[Bảng 4. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống 10](#_Toc116484032)

**DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ**

[Hình 1. Cấu trúc logic của hệ thống A 5](#_Toc519254385)

[Hình 2. Kết nối vật lý của hệ thống A 6](#_Toc519254386)

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

**1. Thông tin Chủ quản hệ thống thông tin**

**- Tên Tổ chức: Tên Chủ quản hệ thống thông tin.**

- Quy định chức năng, nhiệm vụ và quyền hạn: Chủ quản Hệ thống thông tin thực hiện nhiệm vụ, quyền hạn quy định tại …

- Người đại diện: …, Chức vụ: ….

- Địa chỉ: ...

- Thông tin liên hệ:

+ Số điện thoại: …

+ Thư điện tử: …

**2. Thông tin Đơn vị vận hành**

**- Tên Đơn vị vận hành: Tên Đơn vị vận hành** (ví dụ: Sở Thông tin và Truyền Thông tỉnh A)**.**

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số …/QĐ-UBND ngày ../../20xx trích yếu

- Người đại diện: …, Chức vụ: ….

- Địa chỉ: ....

- Thông tin liên hệ:

+ Số điện thoại: …

+ Thư điện tử: …

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

- Phạm vi, quy mô của Hệ thống thông tin A: Hệ thống thông tin của tỉnh A được thiết lập để phục vụ công tác chỉ đạo điều hành và cung cấp dịch vụ công trực tuyến trong phạm vi tỉnh A. Quy mô của hệ thống cung cấp dịch vụ cho hơn 10.000 người sử dụng.

- Đối tượng phục vụ của hệ thống: Cơ quan, tổ chức, doanh nghiệp trên địa bàn tỉnh A.

- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi trung tâm tích hợp dữ liệu:

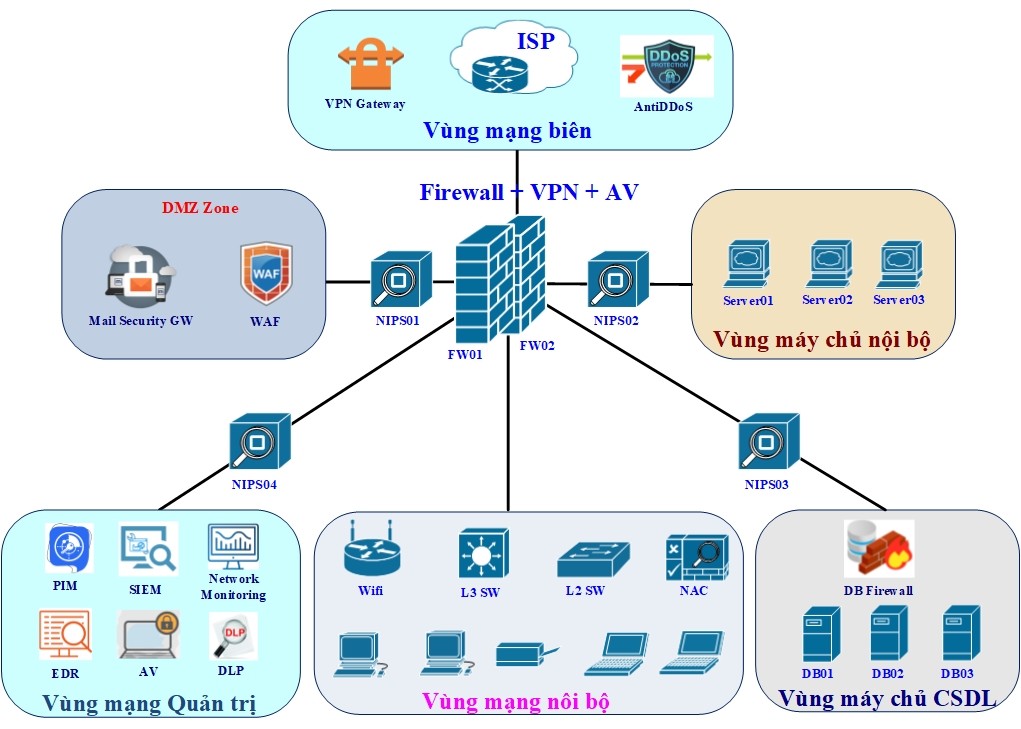
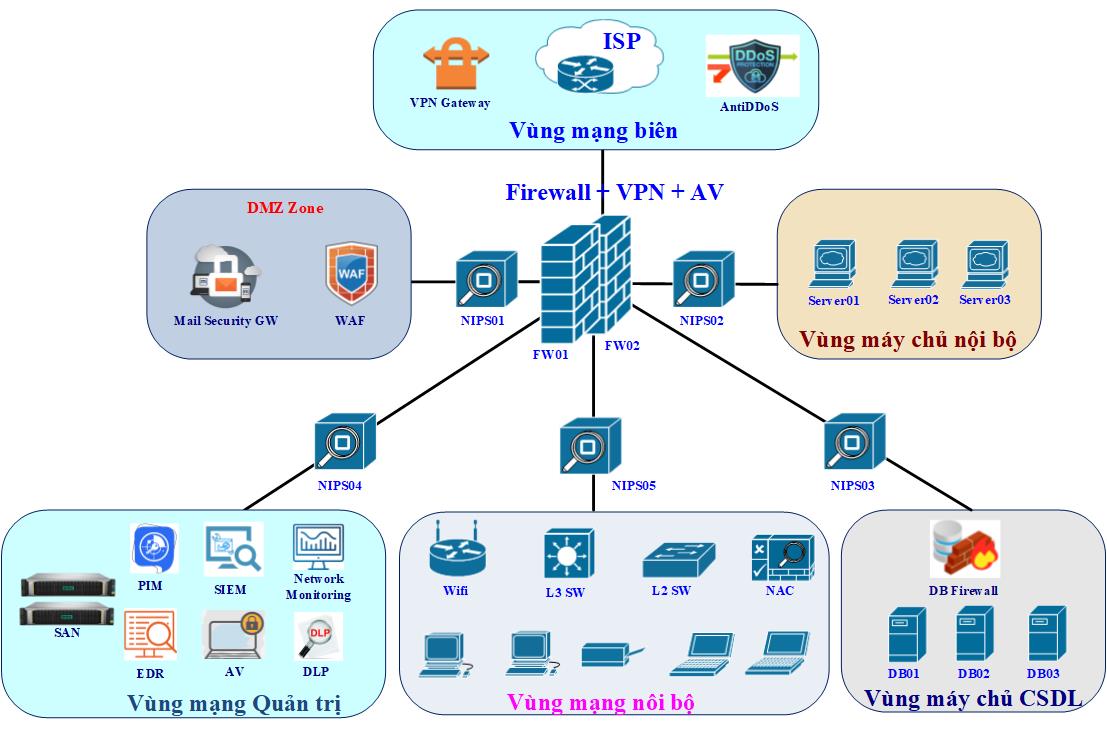
+ Hệ thống cổng thông tin nội bộ.

+ Hệ thống quản lý văn bản.

+ Hệ thống cung cấp dịch vụ công trực tuyến cấp độ 4.

**4. Mô tả cấu trúc của hệ thống**

**4.1. Mô hình logic tổng thể**



Hình 1. Cấu trúc logic của Trung tâm dữ liệu

Các vùng mạng được thiết kế như sau:

- Vùng mạng biên được thiết kế để kết nối hệ thống mạng TTDL ra các mạng bên ngoài và mạng Internet; bảo vệ hệ thống A từ bên ngoài Internet. Vùng mạng này triển khai hệ thống phòng chống tấn công DDoS và Thiết bị cung cấp cổng kết nối VPN.

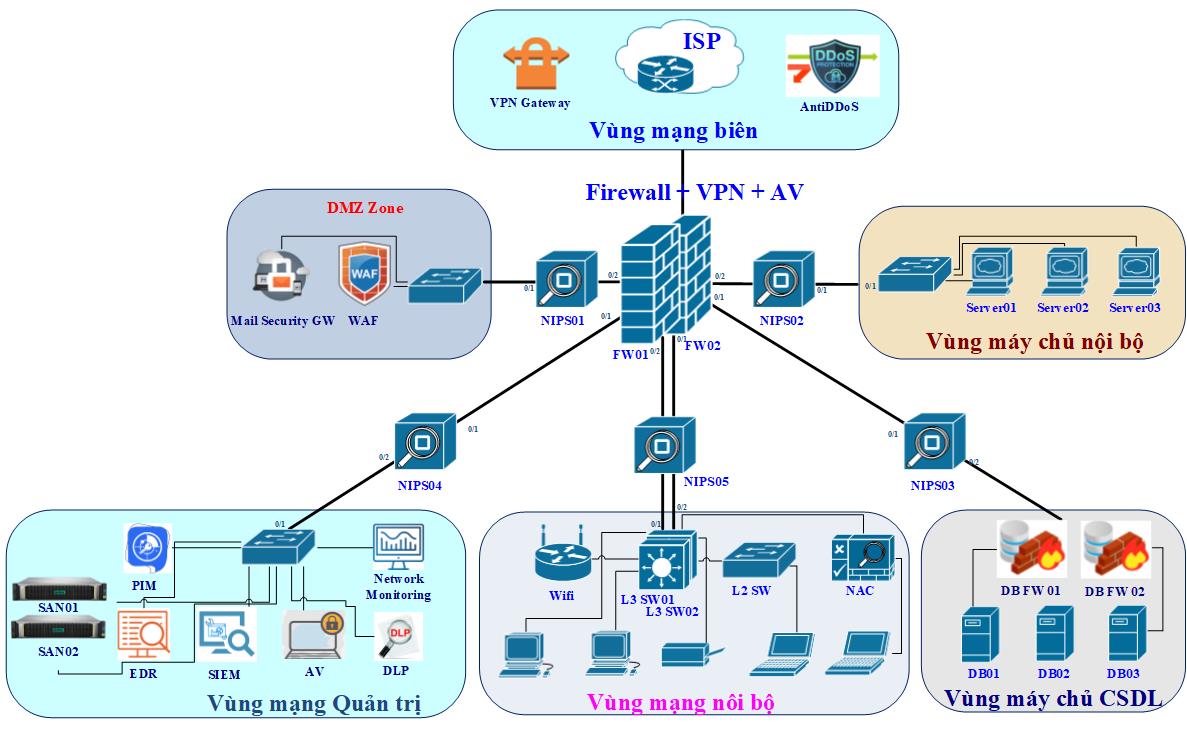
- Vùng DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị Anti-Spam.

- Vùng mạng quản trị đặt các máy chủ quản trị và máy chủ hệ thống.

- Vùng máy chủ nội bộ đặt các máy chủ nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall.

- Vùng máy chủ cơ sở dữ liệu đặt các máy chủ cơ sở dữ liệu phục vụ việc lưu trữ và quản lý cơ sở dữ liệu tập trung trên hệ thống. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị DB Firewall CSDL.

**4.2. Mô hình kết nối vật lý**



Hình 2. Kết nối vật lý của Trung tâm dữ liệu

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên thiết bị/**  **Chủng loại** | **Vị trí triển khai** | **Mục đích sử dụng** |
| 1 | FW01/ Chủng loại | Vùng core | Quản lý truy cập vào/ra và bảo vệ các vùng mạng. |
| 2 | FW02/ Chủng loại | Vùng core | Quản lý truy cập vào/ra và bảo vệ các vùng mạng (Dự phòng nóng cho FW01). |
| 3 | DB FW01/ Chủng loại | Vùng máy chủ CSDL | Quản lý truy cập vào/ra và bảo vệ vùng máy chủ CSDL. |
| 4 | DB FW02/ Chủng loại | Vùng máy chủ CSDL | Quản lý truy cập vào/ra và bảo vệ vùng máy chủ CSDL (Dự phòng nóng cho FW02). |
| 5 | NIPS01/ Chủng loại | Vùng DMZ | Phòng chống xâm nhập vào ra (IPS) giữa internet và vùng DMZ. |
| 6 | NIPS02/ Chủng loại | Vùng máy chủ nội bộ | Phòng chống xâm nhập vào ra (IPS) giữa internet và vùng máy chủ. |
| 7 | NIPS03/ Chủng loại | Vùng máy chủ CSDL | Phòng chống xâm nhập vào ra (IPS) giữa internet và vùng máy chủ CSDL. |
| 8 | NIPS04/ Chủng loại | Vùng mạng Quản trị | Phòng chống xâm nhập vào ra (IPS) giữa internet và vùng mạng quản trị. |
| 9 | NIPS05/ Chủng loại | Vùng mạng nội bộ | Phòng chống xâm nhập vào ra (IPS) giữa internet và vùng mạng nội bộ. |
| 10 | L2 SW/ Chủng loại | Vùng mạng nội bộ | Thiết bị định tuyến vùng mạng nội bộ. |
| 11 | L3 SW01/ Chủng loại | Vùng mạng nội bộ | Thiết bị định tuyến vùng mạng nội bộ. |
| 12 | L3 SW02/ Chủng loại | Vùng mạng nội bộ | Thiết bị định tuyến vùng mạng chủ nội bộ. Dự phòng nóng 1-1 cho L3 SW01/ |
| 13 | SAN01/ Chủng loại | Vùng mạng quản trị | Thiết bị lưu trữ SAN Storage (Tái cấu trúc hệ thống lưu trữ chính, bổ sung năng lực lưu trữ và sử dụng công nghệ lưu trữ tốc độ cao) |
| 14 | SAN02/ Chủng loại | Vùng mạng quản trị | Dự phòng nóng cho SAN01. |

*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*

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Máy chủ/Ứng dụng cài đăt/Vùng mạng/HĐH** | **Mục đích sử dụng** |
| 1 | Cổng thông tin nội bộ | Server01/Cài đặt Web-App /Vùng máy chủ nội bộ/HĐH Centos7 | Cung cấp thông tin công khai cho người sử dụng nội bộ. |
| 2 | Quản lý văn bản | Server02/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7 | Cung cấp ứng dụng quản lý văn bản cho cán bộ bên trong hệ thống. |
| 3 | Dịch vụ công trực tuyến | Server03/Cài đặt Reserver Proxy/Vùng máy chủ nội bộ/HĐH Centos7 | Cung cấp dịch vụ công trực tuyến cho người dân và doanh nghiệp |
| 4 | … | … |  |

*Bảng 3. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống*

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Vùng mạng** | **IP Private** | **IP Public** |
| 1 | DMZ | 192.168.1.0/24 | 202.191.x.0/24 |
| 2 | Vùng mạng quản trị | 192.168.2.0/24 | 202.191.y.0/24 |
| 3 | Vùng máy chủ nội bộ | 192.168.3.0/24 | 202.191.z.0/24 |
| 4 | Vùng máy chủ DB | 192.168.4.0/24 | 202.191.t.0/24 |

*Bảng 4. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống*

**PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT**

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

Hệ thống thông tin của Đơn vị vận hành bao gồm các 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 cổng thông tin nội bộ | 1 | Điều 7/NĐ85 |
| 2 | Hệ thống quản lý văn bản | 2 | Khoản 1/Điều 8/NĐ85 |
| 3 | Hệ thống cung cấp dịch vụ công trực tuyến cấp độ 4 | 3 | Điểm a, khoản 2/Điều 9/NĐ85 |
| 4 | … | … | … |

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

***2.1. Hệ thống mạng LAN nội bộ***

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

***2.2. Hệ thống một cửa điện tử***

Hệ thống quản lý văn bản có xử lý thông tin riêng của Sở TT&TT và phục vụ hoạt động nội bộ cho cán bộ của Sở TT&TT. Căn cứ theo quy định tại Khoản 1/Điều 8/NĐ85, hệ thống này được đề xuất cấp độ 2.

***2.3. Hệ thống cung cấp dịch vụ công trực tuyến cấp độ 4***

Hệ thống cung cấp dịch vụ công trực tuyến cấp độ 4 cung cấp dịch vụ trực tuyến cho người dân, doanh nghiệp với quy mô cung cấp dịch vụ cho hơn 10.000 sử dụng. Căn cứ theo quy định tại điểm a hoặc c, khoản 2/Điều 9/NĐ85, hệ thống được đề xuất cấp độ 3.

**PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM**

**AN TOÀN HỆ THỐNG THÔNG TIN**

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

1. Thiết lập chính sách an toàn thông tin

2. Tổ chức bảo đảm an toàn thông tin

3. Bảo đảm nguồn nhân lực

4. Quản lý thiết kế, xây dựng hệ thống

5. Quản lý vận hành hệ thống

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

- Quản lý an toàn thiết bị đầu cuối

- Quản lý phòng chống phần mềm độc hại

- Quản lý giám sát an toàn hệ thống thông tin

- Quản lý điểm yếu an toàn thông tin

- 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.

**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. Phòng chống phần mềm độc hại trên môi trường mạng

1.7. 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. Bảo mật thông tin liên lạc

3.5. Chống chối bỏ

4. Bảo đảm an toàn dữ liệu

4.1. Nguyên vẹn dữ liệu

4.2. Bảo mật dữ liệu

4.3. Sao lưu dự phòng

Đối với các yêu cầu kỹ thuật chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, Đơn vị vận hành sẽ triển khai nâng cấp, thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong vòng 18 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Thuyết minh phương án bảo đảm an toàn thông tin về quản lý đưa ra các quy định liên quan đến con người và quy trình. Các yêu cầu quản lý ở cấp độ cao hơn khi được đáp ứng thì cũng đáp ứng các yêu cầu ở cấp độ thấp hơn. Do đó, thuyết minh phương án bảo đảm an toàn thông tin về quản lý được thuyết minh chung tại Phụ lục I.

Đối với hạ tầng, thiết bị hệ thống, máy chủ dùng chung để bảo vệ nhiều hệ thống thành phần khác nhau, thì hạ tầng, thiết bị hệ thống, máy chủ đó phải được thiết kế, thiết lập để đáp ứng yêu cầu của hệ thống thành phần có cấp độ cao nhất để bảo đảm an toàn thông tin cho cả hệ thống. Do đó, phải thuyết minh phương án bảo đảm an toàn thông tin về kỹ thuật theo cấp độ 3.

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho trung tâm tích hợp dữ liệu của tỉnh A sẽ bao gồm các nội dung sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hệ thống** | **Cấp độ đề xuất** | **Nội dung thuyết minh** |
| 1 | Thuyết minh phương án đáp ứng yêu cầu quản lý | 3 | Phụ lục I |
| 2 | Thuyết minh phương án đáp ứng yêu cầu kỹ thuật | 3 | Phụ lục II |

**PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 3**

**7.1.1. Thiết lập chính sách an toàn thông tin:**

**7.1.1.1. Chính sách an toàn thông tin**

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.1.1.a** | Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin |
| **Hiện trạng** | Đáp ứng. Quy định tại Điều … Quy chế Bảo đảm an toàn cho hệ thống thông tin … trong hoạt động của công ty Đơn vị vận hành (Quy chế An toàn thông tin) |
| **Phương án** | Điều 3. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin  1. Mục tiêu bảo đảm an toàn thông tin  Bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của Hệ thống … của Đơn vị vận hành.  2. Nguyên tắc  a) Cơ quan, tổ chức thuộc đối tượng áp dụng Quy chế này có trách nhiệm bảo đảm an toàn thông tin và hệ thống thông tin trong phạm vi xử lý công việc của mình theo quy định của pháp luật, hướng dẫn của cơ quan, đơn vị có thẩm quyền và các quy định tại Quy chế này.  b) Bảo đảm an toàn thông tin (ATTT) là yêu cầu bắt buộc, phải được thực hiện thường xuyên, liên tục trong quá trình:  i. Thu thập, tạo lập, xử lý, truyền tải, lưu trữ và sử dụng thông tin, dữ liệu.  ii. Thiết kế, thiết lập và vận hành, nâng cấp, hủy bỏ hệ thống thông tin.  c) Việc bảo đảm an toàn thông tin cho Hệ thống … của Đơn vị vận hành được thực hiện một cách tổng thể, đồng bộ, tập trung trong việc đầu tư các giải pháp bảo vệ, có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp. |
| **Yêu cầu**  **7.1.1.1.b** | Xác định trách nhiệm của đơn vị chuyên trách về an toàn thông tin, các cán bộ làm về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin. |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Điều … Quy chế An toàn thông tin. |
| **Phương án** | Phương án theo Điều … của Quyết định số 1512/QĐ-BTTTT ngày 05/10/2021 của Bộ trưởng Chủ quản Hệ thống thông tin về việc ban hành Quy chế bảo đảm an toàn thông tin mạng. |
| **Yêu cầu**  **7.1.1.1.c** | Xác định phạm vi chính sách an toàn thông tin  1. Phạm vi quản lý về vật lý và logic của tổ chức.  2. Các ứng dụng, dịch vụ hệ thống cung cấp.  3. Nguồn nhân lực đảm bảo an toàn thông tin. |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Điều 1 Quy chế An toàn thông tin |
| **Phương án** | Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng  1. Phạm vi điều chỉnh  Quy chế này quy định các chính sách quản lý và các biện pháp nhằm bảo đảm an toàn thông tin cho Hệ thống … của Đơn vị vận hành.  2. Đối tượng áp dụng  a) Các cán bộ thuộc Đơn vị vận hành;  b) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng Hệ thống … của Đơn vị vận hành;  c) Cơ quan, tổ chức, cá nhân cung cấp dịch vụ công nghệ thông tin và an toàn thông tin mạng phục vụ hoạt động của Hệ thống … của Đơn vị vận hành. |
| **Yêu cầu**  **7.1.1.1.d** | Xây dựng chính sách an toàn thông tin bao gồm:  - Quản lý an toàn mạng;  - Quản lý an toàn máy chủ và ứng dụng;  - Quản lý an toàn dữ liệu;  - Quản lý an toàn thiết bị đầu cuối;  - Quản lý phòng chống phần mềm độc hại;  - Quản lý điểm yếu an toàn thông tin;  - Quản lý giám sát an toàn hệ thống thông tin;  - Quản lý an toàn người sử dụng đầu cuối |
| **Hiện trạng** | Đáp ứng. Đã quy định từ Điều …-… Quy chế An toàn thông tin |
| **Phương án** | **Điều 8. Quản lý an toàn máy chủ và ứng dụng**  1. 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) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;  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.  2. 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.  3. 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.  4. 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.  **Điều 9. Quản lý an toàn dữ liệu**  1. 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.  **Điều 10. Quản lý an toàn thiết bị đầu cuối**  Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:  a) Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lý và cập nhật.  b) Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.  c) Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt.  **Điều 11. Quản lý phòng chống phần mềm độc hại**  1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.  2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.  3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.  4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.  **Điều 12. Quản lý giám sát an toàn hệ thống thông tin**  1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.  2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.  3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT.  **Điều 13. Quản lý điểm yếu an toàn thông tin**  1. Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); Phân loại mức độ nguy hiểm của điểm yếu; Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu.  2. Báo cáo Lãnh đạo/Cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.  3. Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại.  4. Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết.  5. Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.  6. Định kỳ 1 năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống.  **Điều 14. Quản lý sự cố an toàn thông tin**  1. 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.  2. 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.  3. 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.  4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.  5. 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. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo.  **Điều 15. Quản lý an toàn người sử dụng đầu cuối**  1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống  a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.  b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.  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.  2. Trong quá trình sử dụng  a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.  b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.  c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.  d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.  **Điều 16. Kiểm tra, đánh giá và quản lý rủi ro an toàn thông tin**  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, điểm yếu, thử nghiệm xâm nhập 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. |

**7.1.1.2. Xây dựng và công bố**

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.1.2.a** | Chính sách được tổ chức/bộ phận được ủy quyền thông qua trước khi công bố áp dụng |
| **Hiện trạng** | Đáp ứng. Quy chế An toàn thông tin được thông qua trước khi công bố theo quy định. |
| **Phương án** | Xây dựng và công bố Quy chế bảo đảm an toàn thông tin:  1. Quy chế được lấy ý kiến cấp có thẩm quyền, đơn vị liên quan trước khi công bố áp dụng  2. Quy chế được Đơn vị vận hành xây dựng trình Chủ quản Hệ thống thông tin ban hành. |
| **Yêu cầu**  **7.1.1.2.b** | Chính sách được công bố trước khi áp dụng |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Điều 21 Quy chế An toàn thông tin |
| **Phương án** | **Điều 21. Tổ chức triển khai Quy chế**  a) Quy định này có hiệu lực thi hành kể từ ngày ký ban hành.  b) Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các đơn vị liên quan phản ánh kịp thời về Đơn vị chuyên trách để xem xét, bổ sung, sửa đổi. |

**7.1.1.3. Rà soát, sửa đổi**

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.1.3** | Định kỳ 02 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. |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Điều 22 Quy chế An toàn thông tin |
| **Phương án** | **Điều 22. Rà soát, cập nhật, bổ sung Quy chế**  1. Định kỳ 02 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung.  2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Đơn vị chuyên trách về ATTT để tổng hợp báo cáo Chủ quản Hệ thống thông tin điều chỉnh, bổ sung. |

**7.1.2. Tổ chức bảo đảm an toàn thông tin**

**7.1.2.1. 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. Đã quy định tại Điều 5 Quy chế An toàn thông tin |
| **Phương án** | **Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền**  1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:  a) Chủ quản Hệ thống thông tin giao Đơn vị chuyên trách về an toàn thông tin là đầu mối liên hệ, phối hợp với 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 … của Đơn vị vận hành.  b) Đơn vị chuyên trách về an toàn thông tin làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của Hệ thống … của Đơn vị vận hành.  2. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng. |
| **Yêu cầu** | Phân định vai trò, trách nhiệm, cơ chế phối hợp của các bộ phận, cán bộ trong đơn vị chuyên trách về an toàn thông tin. |
| **Hiện trạng** | Chưa đáp ứng |
| **Phương án** | Sẽ xây dựng và bổ sung phương án vào Quy chế An toàn thông tin |

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

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.2.2.a** | Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Điều 5 Quy chế An toàn thông tin |
| **Phương án** | **Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền**  1. Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin:  a) Chủ quản Hệ thống thông tin giao Đơn vị chuyên trách về an toàn thông tin là đầu mối liên hệ, phối hợp với 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 … của Đơn vị vận hành.  b) Đơn vị chuyên trách về an toàn thông tin làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của Hệ thống … của Đơn vị vận hành.  2. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng. |
| **Yêu cầu**  **7.1.2.2.b** | Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Điều 5 Quy chế An toàn thông tin |
| **Phương án** | **Điều 5. Phối hợp với những cơ quan/tổ chức có thẩm quyền**  2. Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin: Tùy theo mức độ sự cố, phối hợp với các đơn vị có liên quan hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng. |
| **Yêu cầu**  **7.1.2.2.c** | Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền |
| **Hiện trạng** | Chưa đáp ứng |
| **Phương án** | Sẽ xây dựng và bổ sung phương án vào Quy chế An toàn thông tin |

**7.1.3. Tổ chức bảo đảm an toàn thông tin**

**7.1.3.1. Tuyển dụng**

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.3.1.a** | Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành về lĩnh vực công nghệ thông tin, an toàn thông tin, phù hợp với vị trí tuyển dụng |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Điều 6 Quy chế An toàn thông tin |
| **Phương án** | **Điều 6. Bảo đảm nguồn nhân lực**  1. 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  2. Xây dựng quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.  3. Xây dựng kế hoạch và định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng.  4. 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.  5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:  a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chứ.  b) 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.  c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. |
| **Yêu cầu**  **7.1.3.1.b** | Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Điều 6 Quy chế An toàn thông tin |
| **Phương án** | **Điều 6. Bảo đảm nguồn nhân lực**  1. 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  2. Xây dựng quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.  3. Xây dựng kế hoạch và định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng.  4. 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.  5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:  a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chứ.  b) 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.  c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. |

**7.1.3.2. Trong quá trình làm việc**

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.3.2.a** | Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống |
| **Hiện trạng** | Đã quy định tại Điều 6 Quy chế An toàn thông tin |
| **Phương án** | **Điều 6. Bảo đảm nguồn nhân lực**  1. 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  2. Xây dựng quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.  3. Xây dựng kế hoạch và định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng.  4. 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.  5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:  a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chứ.  b) 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.  c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. |
| **Yêu cầu**  **7.1.3.2.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. |
| **Hiện trạng** | Đã quy định tại khoản 3, Điều 6 Quy chế An toàn thông tin |
| **Phương án** | **Điều 6. Bảo đảm nguồn nhân lực**  3. Xây dựng kế hoạch và định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng. |
| **Yêu cầu**  **7.1.3.2.c** | Định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng. |
| **Hiện trạng** | Đã quy định tại khoản 3 Điều 6 Quy chế An toàn thông tin |
| **Phương án** | **Điều 6. Bảo đảm nguồn nhân lực**  3. Xây dựng kế hoạch và định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin cho người sử dụng. |

**7.1.3.3. Chấm dứt hoặc thay đổi công việc**

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.3.3.a** | Cán bộ chấm dứt hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 5, Mục a, Điều 6 Quy chế An toàn thông tin |
| **Phương án** | **Điều 6. Bảo đảm nguồn nhân lực**  5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:  a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chứ.  b) 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.  c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. |
| **Yêu cầu**  **7.1.3.3.b** | Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc |
| **Hiện trạng** | Đáp ứng một phần, sẽ bổ sung quy trình trong thời gian 6 tháng tới. Đã quy định tại Khoản 5, Mục b, c, Điều 6 Quy chế An toàn thông tin |
| **Phương án** | **Điều 6. Bảo đảm nguồn nhân lực**  5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:  a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chứ.  b) 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.  c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. |
| **Yêu cầu**  **7.1.3.3.c** | Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. |
| **Hiện trạng** | Đáp ứng một phần, sẽ bổ sung quy trình trong thời gian 6 tháng tới. Đã quy định tại Khoản 5, Mục b, c, Điều 6 Quy chế An toàn thông tin |
| **Phương án** | **Điều 6. Bảo đảm nguồn nhân lực**  5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:  a) Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chứ.  b) 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.  c) Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc. |

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

**7.1.4.1. Thiết kế an toàn hệ thống thông tin**

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.4.1.a** | Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 1, Mục a, b Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  1. Thiết kế an toàn hệ thống thông tin  a) 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.  b) Yêu cầu phải có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.  c) Yêu cầu phải có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.  d) Yêu cầu phải có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.  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**  **7.1.4.1.b** | Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 1, Mục a, b Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  1. Thiết kế an toàn hệ thống thông tin  a) 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.  b) Yêu cầu phải có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.  c) Yêu cầu phải có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.  d) Yêu cầu phải có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.  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**  **7.1.4.1.c** | Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 1, Mục c, d Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  1. Thiết kế an toàn hệ thống thông tin  a) 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.  b) Yêu cầu phải có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.  c) Yêu cầu phải có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.  d) Yêu cầu phải có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.  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**  **7.1.4.1.d** | Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 1, Mục c, d Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  1. Thiết kế an toàn hệ thống thông tin  a) 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.  b) Yêu cầu phải có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.  c) Yêu cầu phải có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.  d) Yêu cầu phải có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.  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**  **7.1.4.1.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. |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 1, Mục đ Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  1. Thiết kế an toàn hệ thống thông tin  a) 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.  b) Yêu cầu phải có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.  c) Yêu cầu phải có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.  d) Yêu cầu phải có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.  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. |

**7.1.4.2. Phát triển phần mềm thuê khoán**

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.4.2.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 |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 2, Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  **2. Phát triển phần mềm thuê khoán**  a) 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.  b) 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.  c) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng.  d) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng. |
| **Yêu cầu**  **7.1.4.2.b** | Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 2, Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  **2. Phát triển phần mềm thuê khoán**  a) 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.  b) 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.  c) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng.  d) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng. |
| **Yêu cầu**  **7.1.4.2.c** | Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 2, Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  **2. Phát triển phần mềm thuê khoán**  a) 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.  b) 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.  c) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng.  d) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng. |
| **Yêu cầu**  **7.1.4.2.d** | Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng. |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 2, Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  **2. Phát triển phần mềm thuê khoán**  a) 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.  b) 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.  c) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc kiểm thử phần mềm trên môi trường thử nghiệm và nghiệm thu trước khi đưa vào sử dụng.  d) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng. |

**7.1.4.3. Thử nghiệm và nghiệm thu hệ thống**

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.4.3.a** | Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng |
| **Hiện trạng** | Đáp ứng một phần. Sẽ bổ sung quy trình trong thời gian 6 tháng tới. Đã quy định tại Mục 3, Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  3. Thử nghiệm và nghiệm thu hệ thống  a) 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.  b) 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.  c) 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.  d) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.  đ) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng? |
| **Yêu cầu**  **7.1.4.3.b** | Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống |
| **Hiện trạng** | Đáp ứng một phần. Sẽ bổ sung quy trình trong thời gian 6 tháng tới. Đã quy định tại Mục 3, Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  3. Thử nghiệm và nghiệm thu hệ thống  a) 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.  b) 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.  c) 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.  d) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.  đ) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng? |
| **Yêu cầu**  **7.1.4.3.c** | Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống |
| **Hiện trạng** | Đáp ứng một phần. Sẽ bổ sung quy trình trong thời gian 6 tháng tới. Đã quy định tại Mục 3, Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  3. Thử nghiệm và nghiệm thu hệ thống  a) 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.  b) 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.  c) 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.  d) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.  đ) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng? |
| **Yêu cầu**  **7.1.4.3.d** | Có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống |
| **Hiện trạng** | Đáp ứng một phần. Sẽ bổ sung quy trình trong thời gian 6 tháng tới. Đã quy định tại Mục 3, Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  3. Thử nghiệm và nghiệm thu hệ thống  a) 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.  b) 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.  c) 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.  d) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.  đ) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng? |
| **Yêu cầu**  **7.1.4.3.đ** | Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng. |
| **Hiện trạng** | Đáp ứng một phần. Sẽ bổ sung quy trình trong thời gian 6 tháng tới. Đã quy định tại Mục 3, Điều 17 Quy chế An toàn thông tin |
| **Phương án** | **Điều 17. Quản lý thiết kế, xây dựng hệ thống**  3. Thử nghiệm và nghiệm thu hệ thống  a) 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.  b) 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.  c) 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.  d) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc đơn vị thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.  đ) Yêu cầu nội dung quy chế bảo đảm ATTT hiện tại phải có quy định về việc có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng? |

**7.1.5. Quản lý vận hành hệ thống thông tin**

**7.1.5.1. 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.

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.5.1.a** | Chính sách và quy trình quản lý an toàn mạng bao gồm:  Quản lý, vận hành hoạt động bình thường của hệ thống |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 1, Điều 7 Quy chế An toàn thông tin |
| **Phương án** | **Điều 7. Quản lý an toàn mạng**  1. 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) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;  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. |
| **Yêu cầu**  **7.1.5.1.b** | Chính sách và quy trình quản lý an toàn mạng bao gồm:  Cập nhật, sao lưu dự phòng và khôi phục hệ thống sau khi xảy ra sự cố |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 2, Điều 7 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 7. Quản lý an toàn mạng**  2. 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. |
| **Yêu cầu**  **7.1.5.1.c** | Chính sách và quy trình quản lý an toàn mạng bao gồm:  Truy cập và quản lý cấu hình hệ thống |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 3, Điều 7 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 7. Quản lý an toàn mạng**  3. Truy cập và quản lý cấu hình hệ thống  a) 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.  b) Cán bộ quản lý, nhân viên vận hành có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, báo cáo cho cán bộ quản lý để tiến hành ngăn chặn, thu hồi, khóa quyền truy cập của các tài khoản vi phạm.  c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác.  d) Quy trình kết nối thiết bị đầu cuối của người sử dụng vào hệ thống mạng; truy nhập và quản lý cấu hình hệ thống; cấu hình tối ưu, tăng cường bảo mật cho thiết bị mạng, bảo mật (cứng hóa) trong hệ thống và thực hiện quy trình trước khi đưa hệ thống vào vận hành khai thác. |
| **Yêu cầu**  **7.1.5.1.d** | Chính sách và quy trình quản lý an toàn mạng bao gồm:  Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại điểm c, Khoản 3, Điều 7 Quy chế An toàn thông tin |
| **Phương án** | **Điều 7. Quản lý an toàn mạng**  3. Truy cập và quản lý cấu hình hệ thống  c) Cấu hình tối ưu, tăng cường bảo mật cho thiết bị hệ thống (cứng hóa) trước khi đưa vào vận hành, khai thác. |

**7.1.5.2. 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.

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.5.2.a** | Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:  Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ. |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 1, Điều 8 Quản lý an toàn máy chủ và ưng dụng |
| **Phương án** | **Điều 8. Quản lý an toàn máy chủ và ứng dụng**  1. 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) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;  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. |
| **Yêu cầu**  **7.1.5.2.b** | Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:  Truy cập mạng của máy chủ |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 2, Điều 8 Quản lý an toàn máy chủ và ứng dụng |
| **Phương án** | **Điều 8. Quản lý an toàn máy chủ và ứng dụng**  2. 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. |
| **Yêu cầu**  **7.1.5.2.c** | Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm: Truy cập và quản trị máy chủ và ứng dụng |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 3, Điều 8 Quản lý an toàn máy chủ và ứng dụng. |
| **Phương án** | **Điều 8. Quản lý an toàn máy chủ và ứng dụng**  3. 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. |
| **Yêu cầu**  **7.1.5.2.d** | Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:  Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 4, Điều 8 Quản lý an toàn máy chủ và ứng dụng |
| **Phương án** | **Điều 8. Quản lý an toàn máy chủ và ứng dụng**  4. 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. |
| **Yêu cầu**  **7.1.5.2.đ** | Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:  Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại điểm d, đ, e, Khoản 1, Điều 8 Quản lý an toàn máy chủ và ứng dụng |
| **Phương án** | **Điều 8. Quản lý an toàn máy chủ và ứng dụng**  1. Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ  d) Có phương án cập nhật bản vá, xử lý điểm yếu an toàn thông tin cho hệ điều hành và các dịch vụ hệ thống trên máy chủ;  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. |
| **Yêu cầu**  **7.1.5.2.e** | Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:  Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 2, Điều 8 Quản lý an toàn máy chủ và ứng dụng |
| **Phương án** | **Điều 8. Quản lý an toàn máy chủ và ứng dụng**  2. 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. |
| **Yêu cầu**  **7.1.5.2.g** | Chính sách và quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:  Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác. |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 3, Điều 8 Quản lý an toàn máy chủ và ứng dụng |
| **Phương án** | **Điều 8. Quản lý an toàn máy chủ và ứng dụng**  3. 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. |

**7.1.5.3. 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.

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.5.3.a** | Chính sách, quy trình quản lý an toàn dữ liệu bao gồm:  Xây dựng và thực thi chính sách, quy trình dự phòng và khôi phục dữ liệu |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 9 Quản lý an toàn dữ liệu |
| **Phương án** | **Điều 9. Quản lý an toàn dữ liệu**  1. 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. |
| **Yêu cầu**  **7.1.5.3.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. |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 4, Điều 9 Quản lý an toàn dữ liệu |
| **Phương án** | **Điều 9. Quản lý an toàn 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. |

**7.1.5.4. Quản lý an toàn thiết bị 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 thiết bị 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.

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.6.4.a** | Chính sách quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:  Quản lý, vận hành hoạt động bình thường cho thiết bị đầu cuối |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại điểm a, b, Điều 10 Quản lý an toàn thiết bị đầu cuối |
| **Phương án** | **Điều 10. Quản lý an toàn thiết bị đầu cuối**  Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:  a) Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lýb và cập nhật.  b) Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn. |
| **Yêu cầu**  **7.1.6.4.b** | Kết nối, truy cập và sử dụng thiết bị đầu cuối từ xa |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại điểm a, b, Điều 10 Quản lý an toàn thiết bị đầu cuối |
| **Phương án** | **Điều 10. Quản lý an toàn thiết bị đầu cuối**  Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:  a) Thông tin về thiết bị đầu cuối (tên, chủng loại, địa chỉ MAC, địa chỉ IP) phải được quản lýb và cập nhật.  b) Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn. |
| **Yêu cầu**  **7.1.6.4.c** | Chính sách quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:  Cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản c Điều 10 Quản lý an toàn thiết bị đầu cuối |
| **Phương án** | **Điều 10: Quản lý an toàn thiết bị đầu cuối**  Quy định về quản lý an toàn thiết bị đầu cuối bao gồm các nội dung:  c) Việc cài đặt, kết nối và gỡ bỏ thiết bị đầu cuối trong hệ thống phải được cho phép bởi người có thẩm quyền và thực hiện theo quy trình được phê duyệt. |

**7.1.5.5. Quản lý phòng chống phần mềm độc hại**

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý phòng chống phần mềm độc hại. 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**  **7.1.5.5.a** | Chính sách quy trình quản lý phòng chống phần mềm độc hại bao gồm:  Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 11 Quản lý phòng chống phần mềm độc hại |
| **Phương án** | **Điều 11. Quản lý phòng chống phần mềm độc hại**  1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.  2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.  3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.  4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống. |
| **Yêu cầu**  **7.1.5.5.b** | Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 11 Quản lý phòng chống phần mềm độc hại |
| **Phương án** | **Điều 11. Quản lý phòng chống phần mềm độc hại**  1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.  2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.  3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.  4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống. |
| **Yêu cầu**  **7.1.5.5.c** | Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 11 Quản lý phòng chống phần mềm độc hại |
| **Phương án** | **Điều 11. Quản lý phòng chống phần mềm độc hại**  1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.  2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.  3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.  4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống. |
| **Yêu cầu**  **7.1.5.5.d** | Định kỳ thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; Thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 11 Quản lý phòng chống phần mềm độc hại |
| **Phương án** | **Điều 11. Quản lý phòng chống phần mềm độc hại**  1. Tất cả các máy trạm, máy chủ phải được trang bị phần mềm phòng chống mã độc. Các phần mềm phòng chống mã độc phải được thiết lập chế độ tự động cập nhật; chế độ tự động quét mã độc khi sao chép, mở các tập tin.  2. Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm phòng chống mã độc, mất dữ liệu,…), người sử dụng phải báo trực tiếp cho bộ phận có trách nhiệm của đơn vị để xử lý.  3. Phần mềm ứng dụng trước khi được cài đặt, sử dụng phải được kiểm tra xem có phần mềm độc hại tồn tại hay không? Tất cả các tập tin, thư mục phải được quét mã độc trước khi sao chép, sử dụng.  4. Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống. |

**7.1.5.6. Quản lý giám sát an toàn hệ thống thông tin**

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý giám sát. 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**  **7.1.5.6.a** | Chính sách, quy trình quản lý giám sát an toàn hệ thống thông tin bao gồm:  Quản lý, vận hành hoạt động bình thường của hệ thống giám sát |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 12 Quy chế An toàn thông tin |
| **Phương án** | **Điều 12. Quản lý giám sát an toàn hệ thống thông tin**  1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.  2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.  3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. |
| **Yêu cầu**  **7.1.5.6.b** | Đối tượng giám sát bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có) |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 12 Quy chế An toàn thông tin |
| **Phương án** | **Điều 12. Quản lý giám sát an toàn hệ thống thông tin**  1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.  2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.  3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. |
| **Yêu cầu**  **7.1.5.6.c** | Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 12 Quy chế An toàn thông tin |
| **Phương án** | **Điều 12. Quản lý giám sát an toàn hệ thống thông tin**  1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.  2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.  3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. |
| **Yêu cầu**  **7.1.5.6.d** | Truy cập và quản trị hệ thống giám sát |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 12 Quy chế An toàn thông tin |
| **Phương án** | **Điều 12. Quản lý giám sát an toàn hệ thống thông tin**  1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.  2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.  3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. |
| **Yêu cầu**  **7.1.5.6.đ** | Loại thông tin cần được giám sát |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 12 Quy chế An toàn thông tin |
| **Phương án** | **Điều 12. Quản lý giám sát an toàn hệ thống thông tin**  1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.  2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.  3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. |
| **Yêu cầu**  **7.1.5.6.e** | Lưu trữ và bảo vệ thông tin giám sát (nhật ký hệ thống) |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 12 Quy chế An toàn thông tin |
| **Phương án** | **Điều 12. Quản lý giám sát an toàn hệ thống thông tin**  1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.  2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.  3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. |
| **Yêu cầu**  **7.1.5.6.g** | Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 12 Quy chế An toàn thông tin |
| **Phương án** | **Điều 12. Quản lý giám sát an toàn hệ thống thông tin**  1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.  2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.  3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. |
| **Yêu cầu**  **7.1.5.6.h** | Theo dõi, giám sát và cảnh báo sự cố phát hiện được trên hệ thống thông tin |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 12 Quy chế An toàn thông tin |
| **Phương án** | **Điều 12. Quản lý giám sát an toàn hệ thống thông tin**  1. Triển khai hệ thống giám sát trung tâm phải đáp ứng yêu cầu tại khoản 1, Điều 5 Thông tư số 31/2017/TT-BTTTT.  2. Thông tin giám sát và danh mục các đối tượng giám sát phải đáp ứng yêu cầu tại khoản 2, Điều 5 Thông tư số 31/2017/TT-BTTTT.  3. Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.  4. Thực thi nhiệm vụ giám sát theo quy định tại khoản 3, Điều 5 Thông tư số 31/2017/TT-BTTTT. |

**7.1.5.7. Quản lý điểm yếu 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 điểm yếu 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**  **7.1.5.7.a** | Chính sách quy trình quản lý điểm yếu an toàn thông tin an toàn thông tin bao gồm:  Quản lý thông tin các thành phần có trong hệ thống có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác (nếu có) |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 1 Điều 13 Quy chế An toàn thông tin |
| **Phương án** | **Điều 13. Quản lý điểm yếu an toàn thông tin**  1. Quản lý thông tin điểm yếu an toàn thông tin đối với từng thành phần có trong hệ thống (hệ điều hành, máy chủ, ứng dụng, dịch vụ…); Phân loại mức độ nguy hiểm của điểm yếu; Xây dựng phương án và quy trình xử lý đối với từng mức độ nguy hiểm của điểm yếu. |
| **Yêu cầu 7.1.5.7.b** | Chính sách quy trình quản lý điểm yếu an toàn thông tin an toàn thông tin bao gồm:  Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong hệ thống đã xác định |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 2, 3 Điều 13 Quy chế An toàn thông tin |
| **Phương án** | **Điều 13: Quản lý điểm yếu an toàn thông tin**  2. Báo cáo Lãnh đạo/Cán bộ quản lý ngay khi phát hiện điểm yếu an toàn thông tin ở mức độ nghiêm trọng. Thực hiện cảnh báo và xử lý điểm yếu an toàn thông tin theo chỉ đạo. Việc xử lý điểm yếu an toàn thông tin phải bảo đảm không làm ảnh hưởng/gián đoạn hoạt động của hệ thống.  3. Xây dựng phương án xử lý tạm thời đối với trường hợp điểm yếu an toàn thông tin chưa được khắc phục và phương án khôi phục hệ thống trong trường hợp xử lý điểm yếu thất bại. |
| **Yêu cầu 7.1.7.7.c** | Chính sách quy trình quản lý điểm yếu an toàn thông tin an toàn thông tin bao gồm:  Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 4 Điều 13 Quy chế An toàn thông tin |
| **Phương án** | **Điều 13. Quản lý điểm yếu an toàn thông tin**  4. Có trách nhiệm phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin đối với các điểm yếu khi cần thiết. |
| **Yêu cầu 7.1.5.7.d** | Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng |
| **Hiện trạng** | Đáp ứng. Đã quy định tại Khoản 5 Điều 13 Quy chế An toàn thông tin |
| **Phương án** | **Điều 13. Quản lý điểm yếu an toàn thông tin**  5. Kiểm tra, đánh giá và xử lý điểm yếu an toàn thông tin cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng. |
| **Yêu cầu 7.1.5.7.đ** | Chính sách quy trình quản lý điểm yếu an toàn thông tin an toàn thông tin bao gồm:  Định kỳ kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Khoản 6 Điều 13 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 13. Quản lý điểm yếu an toàn thông tin**  6. Định kỳ 1 năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ hệ thống thông tin; Thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong hệ thống. |

**7.1.5.8. 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.

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.5.8.a** | Chính sách quy trình quản lý sự cố an toàn thông tin bao gồm:  Phân nhóm sự cố an toàn thông tin |
| **Hiện trạng** | Đáp ứng một phần. Quy định tại Điều 14 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 14. Quản lý sự cố an toàn thông tin**  1. 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.  2. 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.  3. 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.  4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.  5. 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. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo.  Sẽ bổ sung phương án vào dự thảo quy chế An toàn thông tin và ban hành trong vòng 6 tháng kể từ khi HSĐXCĐ được phê duyệt các quy trình:   * Quy trình ứng cứu sự cố an toàn thông tin thông thường * Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng |
| **Yêu cầu**  **7.1.5.8.b** | Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin |
| **Hiện trạng** | Đáp ứng một phần. Quy định tại Điều 14 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 14. Quản lý sự cố an toàn thông tin**  1. 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.  2. 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.  3. 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.  4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.  5. 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. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. |
| **Yêu cầu**  **7.1.5.8.c** | Kế hoạch ứng phó sự cố an toàn thông tin |
| **Hiện trạng** | Đáp ứng một phần. Quy định tại Điều 14 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 14. Quản lý sự cố an toàn thông tin**  1. 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.  2. 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.  3. 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.  4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.  5. 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. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. |
| **Yêu cầu**  **7.1.5.8.d** | Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin |
| **Hiện trạng** | Đáp ứng một phần. Quy định tại Điều 14 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 14. Quản lý sự cố an toàn thông tin**  1. 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.  2. 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.  3. 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.  4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.  5. 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. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. |
| **Yêu cầu**  **7.1.5.8.đ** | Quy trình ứng cứu sự cố an toàn thông tin thông thường |
| **Hiện trạng** | Đáp ứng một phần. Quy định tại Điều 14 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 14. Quản lý sự cố an toàn thông tin**  1. 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.  2. 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.  3. 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.  4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.  5. 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. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. |
| **Yêu cầu**  **7.1.5.8.e** | Quy trình ứng cứu sự cố an toàn thông tin nghiêm trọng |
| **Hiện trạng** | Đáp ứng một phần. Quy định tại Điều 14 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 14. Quản lý sự cố an toàn thông tin**  1. 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.  2. 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.  3. 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.  4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.  5. 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. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. |
| **Yêu cầu**  **7.1.5.8.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 |
| **Hiện trạng** | Đáp ứng một phần. Quy định tại Điều 14 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 14. Quản lý sự cố an toàn thông tin**  1. 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.  2. 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.  3. 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.  4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.  5. 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. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. |
| **Yêu cầu**  **7.1.5.8.h** | Định kỳ tổ chức diễn tập phương án xử lý sự cố an toàn thông tin |
| **Hiện trạng** | Đáp ứng một phần. Quy định tại Điều 14 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 14. Quản lý sự cố an toàn thông tin**  1. 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.  2. 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.  3. 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.  4. Quyết định toàn diện về mặt kỹ thuật đối với các cơ quan trong quá trình khắc phục sự cố về ATTT; Hỗ trợ, phối hợp và hướng dẫn các cơ quan khắc phục sự cố mất ATTT; Yêu cầu ngưng hoạt động một phần hoặc toàn bộ các hệ thống thông tin của các cơ quan nhằm phục vụ công tác khắc phục sự cố về ATTT; Phối hợp với đơn vị chức năng trong điều tra các nguyên nhân gây ra sự cố mất an toàn thông tin theo chỉ đạo của Lãnh đạo.  5. 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. Tổ chức diễn tập phương án xử lý sự cố an toàn thông tin theo chỉ đạo của Lãnh đạo. |

**7.1.5.9. 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.

|  |  |
| --- | --- |
| **Yêu cầu**  **7.1.5.9.a** | Chính sách quy trình quản lý an toàn người sử dụng đầu cuối bao gồm:  Quản lý truy cập, sử dụng tài nguyên nội bộ |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 15 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 15. Quản lý an toàn người sử dụng đầu cuối**  1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống  a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.  b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.  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.  2. Trong quá trình sử dụng  a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.  b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.  c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.  d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.  Sẽ bổ sung quy trình quản lý an toàn người sử dụng vào dự thảo Quy chế an toàn thông tin và ban hành trong vòng 6 tháng kể từ khi HSĐXCP được phê duyệt |
| **Yêu cầu**  **7.1.5.9.b** | Quản lý truy cập mạng và tài nguyên trên Internet |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 15 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 15. Quản lý an toàn người sử dụng đầu cuối**  1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống  a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.  b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.  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.  2. Trong quá trình sử dụng  a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.  b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.  c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.  d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.  Sẽ bổ sung quy trình quản lý an toàn người sử dụng vào dự thảo Quy chế an toàn thông tin và ban hành trong vòng 6 tháng kể từ khi HSĐXCP được phê duyệt |
| **Yêu cầu**  **7.1.5.9.c** | Cài đặt và sử dụng máy tính an toàn |
| **Hiện trạng** | Đáp ứng một phần. Đã quy định tại Điều 15 Quy chế An toàn thông tin. |
| **Phương án** | **Điều 15. Quản lý an toàn người sử dụng đầu cuối**  1. Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống  a) Người sử dụng khi truy cập, sử dụng tài nguyên nội bộ, truy cập mạng và tài nguyên trên Internet phải tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin và các quy định của cơ quan, tổ chức.  b) Khi cài đặt, kết nối máy tính/thiết bị đầu cuối phải thực hiện theo hướng dẫn/quy trình dưới sự giám sát của bộ phận chuyên trách về an toàn thông tin.  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.  2. Trong quá trình sử dụng  a) Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng. Chịu trách nhiệm bảo đảm an toàn thông tin mạng trong phạm vi trách nhiệm và quyền hạn được giao.  b) Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng.  c) Khi phát hiện nguy cơ hoặc sự cố mất an toàn thông tin mạng phải báo cáo ngay với cấp trên và bộ phận phụ trách công nghệ thông tin của cơ quan, đơn vị để kịp thời ngăn chặn và xử lý.  d) Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.  Sẽ bổ sung quy trình quản lý an toàn người sử dụng vào dự thảo Quy chế an toàn thông tin và ban hành trong vòng 6 tháng kể từ khi HSĐXCP được phê duyệt |

**7.1.5.10. 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 … dự thảo Quy chế bảo đảm an toàn, an ninh mạng hệ thống ... |
| **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. |

**7.1.5.11. Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.**

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ |
| **Hiện trạng** | Đáp ứng. Tham chiếu điều … dự thảo Quy chế bảo đảm an toàn, an ninh mạng hệ thống ... |
| **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 CẤP ĐỘ 3**

Trung tâm tích hợp dữ liệu có nhiều hệ thống thành phần khác nhau, trong đó hệ thống thành phần cung cấp dịch vụ công trực tuyến được đề xuất là cấp độ 3 (cấp độ cao nhất). Do đó, ngoài các máy chủ được sử dụng để triển khai hệ thống dịch vụ công trực truyến thì các hệ thống dùng chung với các hệ thống 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 3 như sau:

**1. Bảo đảm an toàn mạng**

***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 | N/A | Vùng mạng nội bộ độc tập, tách riêng khỏi hệ thống của trung tâm dữ liệu |
| 2 | Vùng mạng biên | Có | Kết nối hệ thống với mạng Internet và mạng diện rộng |
| 3 | Vùng DMZ | Có | Vùng máy chủ dịch vụ, cung cấp dịch vụ trực tiếp ra bên ngoài Internet |
| 4 | Vùng máy chủ nội bộ | Có | Vùng máy chủ nội bộ, cung cấp các dịch vụ nội bộ |
| 5 | Vùng mạng máy chủ cơ sở dữ liệu | Có | Lưu trữ và quản lý cơ sở dữ liệu tập trung của các hệ thống thành phần |
| 6 | Vùng mạng không dây | Không có | Trung tâm dữ liệu không cho phép sử dụng mạng không dây |
| 7 | Vùng quản trị | Có | Server Management (Quản lý hạ tầng) cài đặt một tập hợp các công cụ quản trị và giám sát toàn bộ các thiết bị mạng, bảo mật, máy chủ và lưu trữ. |

b) Phương án bảo đảm an toàn thông tin

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn | Có | Các thiết bị hệ thống/máy chủ được thiết lập cấu hình VPN cho phép quản trị từ xa an toàn. |
| 2 | Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập | Có | Hệ thống sử dụng các tường lửa FW01/ Chủng loại và FW02/ Chủng loại; NIPS01/ Chủng loại; NIPS02/ Chủng loại, NIPS03/ Chủng loại, NIPS04/ Chủng loại, NIPS05/ Chủng loại để kiểm soát truy cập và phòng chống xâm nhập giữa các vùng mạng của hệ thống. |
| 3 | Phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính | Có | Các thiết bị mạng chính được thiết kế và cấu hình hoạt động ở chế độ A-A. Cụ thể:  - Firewall: FW01/ Chủng loại; FW02/ Chủng loại (Dự phòng nóng cho FW01)  - DB Firewall: DB FW01/ Chủng loại; DB FW02/ Chủng loại (Dự phòng nóng cho DB FW01)  - Switch: L3 SW01/ Chủng loại; L3 SW02/ Chủng loại (Dự phòng nóng 1-1 cho L3 SW01)  - SAN Storage: SAN01/ Chủng loại; SAN02/ Chủng loại (Dự phòng nóng cho SAN01) |
| 4 | Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu | Có | - Quản lý truy cập CSDL bởi tường lửa DB FW01/ Chủng loại; DB FW02/ Chủng loại  - Không kết nối internet trực tiếp cho các máy chủ CSDL.  - Cài đặt Phần mềm virus và cập nhật định kỳ cho máy chủ CSDL. |
| 5 | Phương án chặn lọc phần mềm độc hại trên môi trường mạng | Có | Hệ thống sử dụng các thiết bị FW01, FW02, license IPS, antivirus, DoS protection trên Firewall để chặn lọc phần mềm độc hại trên môi trường mạng |
| 6 | Phương án phòng chống tấn công từ chối dịch vụ | Có | Hệ thống sử dụng giải pháp AntiDDos được triển khai ở vùng mạng biên để thực hiện phát hiện và phòng chống tấn công DoS/DDoS |
| 7 | Phương án phòng, chống tấn công mạng cho ứng dụng web | Có | Sử dụng sản phẩm Tường lửa ứng dụng web để phòng, chống tấn công cho ứng dụng web |
| 8 | Phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử | Có | Hệ thống sử dụng Giải pháp Email Security Gateway để bảo đảm an toàn thông tin cho hệ thống mail |
| 9 | Phương án quản lý truy cập lớp mạng |  | Hệ thống sử dụng Giải pháp NAC |
| 10 | Phương án giám sát hệ thống thông tin tập trung | Có | Đầu tư giải pháp giám sát hệ thống thông tin tập trung (Network monitoring), để giám sát hiệu năng, trạng thái các thiết bị trong hệ thống. |
| 11 | Phương án giám sát an toàn hệ thống thông tin tập trung | Có | Hệ thống sử dụng giải pháp ArcSight/Splunk/QRadar/LogRhythm được triển khai ở vùng mạng quản trị, cho phép quản trị tập trung nhật ký hệ thống từ các thiết bị/máy chủ |
| 12 | Phương án quản lý sao lưu dự phòng tập trung | Có | Sử dụng hệ thống SAN, có năng lực quản lý và lưu trữ 20T dữ liệu. |
| 13 | Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung | Có | Sử dụng giải pháp AntiVirus có chức năng quản lý tập trung hoặc hệ thống EDR. |
| 14 | Có phương án phòng, chống thất thoát dữ liệu | Có | Sử dụng giải pháp/Thiết bị DLP (Data loss prevention). |
| 15 | Có phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau | Có | Sử dụng đồng thời hai kết nối Internet của hai nhà cung cấp dịch vụ khác nhau để đảm bảo kết nối không bị gián đoạn |
| 16 | Có phương án bảo đảm an toàn cho mạng không dây (nếu có) | N/A |  |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet | Có | Hệ thống được thiết lập trên FW01, FW02 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 | Hệ thống được thiết lập chỉ cho phép kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể.  Chính sách được thiết lập trên FW01 và FW02 theo chiều từ bên ngoài vào vùng DMZ. |
| 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 để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng được thiết lập trên các FW01-02. |
| 4 | Phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý. | Có | Thực hiện chính sách trên thiết bị VPN Gateway tại vùng mạng biên. Mỗi người sử dụng sẽ có tài khoản khác nhau, khi kết nối VPN sẽ nhận được địa chỉ IP và chính sách truy cập vào hệ thống khác nhau. |
| 5 | Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống | Có | Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được thiết lập trên các FW01-02. |

***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 các cặp tương ứng như kiểm soát truy cập từ bên ngoài trên các FW01-02. |
| 2 | Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian | Có | Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian được thiết lập trên FW01 và FW02 |
| 3 | Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chức năng và chính sách của tổ chức | Chưa có | Trung tâm dữ liệu không có vùng mạng nội bộ. Do đó, yêu cầu này sẽ nghiên cứu áp dụng trong trường hợp cụ thể. |

***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 | Lưu trữ và quản lý tập trung nhật ký hệ thống | Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 tháng |
| **Thiết bị** |
| FW01 | + | + | + | + |
| FW02 | + | + | + | + |
| DB FW01 | + | + | + | + |
| DB FW02 | + | + | + | + |
| NIPS01 | + | + | + | + |
| NIPS02 | + | + | + | + |
| NIPS03 | + | + | + | + |
| NIPS04 | + | + | + | + |
| NIPS05 | + | + | + | + |
| L2 SW | + | + | + | + |
| L3 SW01 | + | + | + | + |
| L3 SW02 | + | + | + | + |
| SAN01 | + | + | + | + |
| SAN02 | + | + | + | + |

***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 | Có | Các vùng mạng được triển khai hệ thống NIPS01-05, hoạt động ở chế độ Inline cho phép phát hiện và phòng chống xâm nhập. |
| 2 | Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng | Có | Đã thiết lập chức năng tự động cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng đều được thiết lập trên các thiết bị IDS/IPS NIPS01-05. |
| 3 | Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp | Có | Các IDS/IPS NIPS01-05 có năng lực xử lý đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp. |

***1.6. Phòng chống phần mềm độc hại trên môi trường mạng***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có phương án phòng chống phần mềm độc hại trên môi trường mạng | Có | Chức năng phòng chống phần mềm độc hại trên môi trường mạng được tích hợp trên các Firewall. Các Firewall FW01, FW02 được thiết lập cấu hình để có thể phát hiện ra các hành vi mã độc trên môi trường mạng. |
| 2 | Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại | Có | Đã thiết lập chức năng cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại trên các Firewall FW01, FW02 có tích hợp chức năng phòng chống phần mềm độc hại trên môi trường mạng. |
| 3 | Bảo đảm năng lực hệ thống đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp | Có | Các Firewall FW01, FW02 có tích hợp chức năng phòng chống phần mềm độc hại trên môi trường mạng có năng lực xử lý đáp ứng đủ theo yêu cầu, quy mô số lượng người dùng và dịch vụ, ứng dụng của hệ thống cung cấp. |

***1.7. 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 | Hạn chế được số lần đăng nhập sai | Phân quyền truy cập, quản trị thiết bị | Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng |
| **Thiết bị** |
| FW01 | + | + | + | + | + | + |
| FW02 | + | + | + | + | + | + |
| DB FW01 | + | + | + | + | + | + |
| DB FW02 | + | + | + | + | + | + |
| NIPS01 | + | + | + | + | + | + |
| NIPS02 | + | + | + | + | + | + |
| NIPS03 | + | + | + | + | + | + |
| NIPS04 | + | + | + | + | + | + |
| NIPS05 | + | + | + | + | + | + |
| L2 SW | + | + | + | + | + | + |
| L3 SW01 | + | + | + | + | + | + |
| L3 SW02 | + | + | + | + | + | + |
| SAN01 | + | + | + | + | + | + |
| SAN02 | + | + | + | + | + | + |

**2. Bảo đảm an toàn máy chủ**

***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 | Hạn chế số lần đăng nhập sai | vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định |
| **Máy chủ** |
| Server01/Cài đặt Web-App /Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + | + |
| Server02/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + | + |
| Server03/Cài đặt Reserver Proxy/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + | + |

***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) | Thay đổi cổng quản trị mặc định của máy chủ | Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa |
| **Máy chủ** |
| Server01/Cài đặt Web-App /Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + |
| Server02/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + |
| Server03/Cài đặt Reserver Proxy/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + |

***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 | Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống | Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ | Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng |
| **Máy chủ** |
| Server01/Cài đặt Web-App /Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + | + |
| Server02/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + | + |
| Server03/Cài đặt Reserver Proxy/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + | + |

***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** |
| Server01/Cài đặt Web-App /Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + |
| Server02/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + |
| Server03/Cài đặt Reserver Proxy/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + | + |

***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 | Quản lý tập trung các phần mềm phòng chống mã độc cài đặt trên máy chủ |
| **Máy chủ** |
| Server01/Cài đặt Web-App /Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + |
| Server02/Cài đặt Web-App/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + |
| Server03/Cài đặt Reserver Proxy/Vùng máy chủ nội bộ/HĐH Centos7 | + | + | + |

***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 | Có | Sử dụng giải pháp đi kèm HĐH |
| 2 | Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành | Có | Sử dụng các giải pháp sao lưu trên các hệ thống máy chủ, SAN để thực hiện sao lưu dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành |
| 3 | Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa | Có | Format cấp thấp hệ thiết bị.  Hủy thiết bị cũ/hỏng |

**3. Bảo đảm an toàn ứng dụng**

***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 | Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng | Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng |
| **Ứng dụng** |
| Dịch vụ công trực tuyến | + | + | + | + | + | + |
| Cổng thông tin nội bộ | + | + | + | + | + | + |
| Quản lý văn bản | + | + | + | + | + | + |

***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 | Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với từng người/nhóm sử dụng | Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng |
| **Ứng dụng** |
| Dịch vụ công trực tuyến | + | + | + | + | + |
| Cổng thông tin nội bộ | + | + | + | + | + |
| Quản lý văn bản | + | + | + | + | + |

***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 | Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung | Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng |
| **Ứng dụng** |
| Dịch vụ công trực tuyến | + | + | + |
| Cổng thông tin nội bộ | + | + | + |
| Quản lý văn bản | + | + | + |

***3.4. Bảo mật thông tin liên lạc***

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật. | Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền |
| **Ứng dụng** |
| Dịch vụ công trực tuyến | + | + |
| Cổng thông tin nội bộ | + | + |
| Quản lý văn bản | + | + |

***3.5. Chống chối bỏ***

|  |  |
| --- | --- |
| **Yêu cầu** | Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng |
| **Ứng dụng** |
| Dịch vụ công trực tuyến | + |
| Cổng thông tin nội bộ | + |
| Quản lý văn bản | + |

***3.6. 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 | Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu | Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa | Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF |
| **Ứng dụng** |
| Dịch vụ công trực tuyến | + | + | + | + |
| Cổng thông tin nội bộ | + | + | + | + |
| Quản lý văn bản | + | + | + | + |

**4. Bảo đảm an toàn dữ liệu**

***4.1. Nguyên vẹn dữ liệu***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn | Có | Dữ liệu quan trọng trên hệ thống bao gồm dữ liệu: dữ liệu nghiệp vụ, văn bản điện tử quan trọng và dữ liệu cấu hình hệ thống.  Dữ liệu được nén và được lưu trữ cùng mã kiểm tra MD5 trên hệ thống SAN. |

***4.2. 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 quan trọng trên hệ thống bao gồm dữ liệu: dữ liệu nghiệp vụ, văn bản điện tử quan trọng và dữ liệu cấu hình hệ thống.  Dữ liệu được nén và được lưu trữ mã hóa sử dụng công cụ XXX (hỗ trợ các chuẩn mã hóa: DES, AES,…) trên hệ thống SAN. |

***4.3. 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 | Thông tin, dữ liệu được lưu trữ và quản lý tập trung trên hệ thống lưu trữ SAN. |
| 2 | Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau | Có | Thông tin dữ liệu được phân theo từng nhóm theo đặc trưng nghiệp vụ hoặc chức năng. Được quy định về việc đặt tên các tập tin/thư mục khi lưu trữ trên hệ thống. |
| 3 | Có hệ thống/phương tiện lưu trữ độc lập để sao lưu dự phòng | Có | Hệ thống SAN được phân vùng lưu trữ riêng để phục vụ việc lưu trữ thông tin, dữ liệu. |