|  |
| --- |
| **BỘ Y TẾ**  **CỤC CÔNG NGHỆ THÔNG TIN**  ***HỒ SƠ***  **HỒ SƠ ĐỀ XUẤT CẤP ĐỘ**  **HỆ THỐNG PHẦN MỀM BÁO CÁO BỆNH KHÔNG LÂY NHIỄM**  **BỘ Y TẾ - 2022** |

**MỤC LỤC**

[THUẬT NGỮ, TỪ VIẾT TẮT 1](#_Toc87361741)

[**DANH MỤC CÁC BẢNG** 2](#_Toc87361742)

[**DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ** 3](#_Toc87361743)

[**PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN** 4](#_Toc87361744)

[**1. Thông tin Chủ quản hệ thống thông tin** 4](#_Toc87361745)

[**2. Thông tin Đơn vị vận hành** 4](#_Toc87361746)

[**3. Mô tả phạm vi, quy mô của hệ thống** 4](#_Toc87361747)

[**4. Mô tả cấu trúc của hệ thống** 5](#_Toc87361748)

[**4.1. Sơ đồ logic tổng thể** 5](#_Toc87361749)

[**4.2. Sơ đồ kết nối vật lý** 7](#_Toc87361750)

[**4.3. Danh mục thiết bị sử dụng trong hệ thống** 7](#_Toc87361751)

[**4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống** 9](#_Toc87361752)

[**4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống** 10](#_Toc87361753)

[**PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT** 11](#_Toc87361754)

[**1. Danh mục hệ thống thông tin và cấp độ đề xuất** 11](#_Toc87361755)

[**2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin** 11](#_Toc87361756)

[**PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM** 13](#_Toc87361757)

[**AN TOÀN HỆ THỐNG THÔNG TIN** 13](#_Toc87361758)

[**PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 3** 16](#_Toc87361759)

[**1. Thiết lập chính sách an toàn thông tin** 16](#_Toc87361760)

[**2. Tổ chức bảo đảm an toàn thông tin** 17](#_Toc87361761)

[**3. Tổ chức bảo đảm an toàn thông tin** 17](#_Toc87361762)

[**4. Quản lý thiết kế, xây dựng hệ thống thông tin** 18](#_Toc87361763)

[**5. Quản lý vận hành hệ thống thông tin** 19](#_Toc87361764)

[**PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN ĐÁP ỨNG YÊU CẦU KỸ THUẬT** 21](#_Toc87361765)

[**1. Bảo đảm an toàn mạng** 21](#_Toc87361766)

[**2. Bảo đảm an toàn máy chủ** 29](#_Toc87361767)

[**3. Bảo đảm an toàn ứng dụng** 34](#_Toc87361768)

[**4. Bảo đảm an toàn dữ liệu** 37](#_Toc87361769)

# 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 7](#_Toc519254382)

[Bảng 2. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống 8](#_Toc519254383)

[Bảng 3. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống 8](#_Toc519254384)

**DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ**

[Hình 1. Cấu trúc logic của hệ thống thông tin của Bộ Y tế 5](#_Toc519254385)

[Hình 2. Kết nối vật lý của hệ thống thông tin của Bộ Y tế 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: Trung tâm Dữ liệu y tế**

- Quy định chức năng, nhiệm vụ và quyền hạn:

- Người đại diện: Giám đốc Trung tâm.

- Địa chỉ: 135 Núi Trúc – Ba Đình – Hà Nội

- Thông tin liên hệ: 0243.7368.315

**2. Thông tin Đơn vị vận hành**

**- Tên Đơn vị vận hành: Trung tâm Dữ liệu y tế**

- Quy định chức năng, nhiệm vụ và quyền hạn:

- Người đại diện: Giám đốc Trung tâm.

- Địa chỉ: 135 Núi Trúc – Ba Đình – Hà Nội

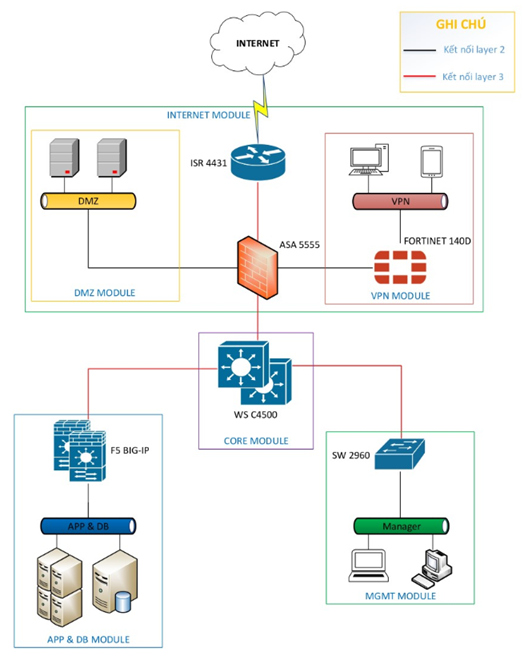
- Thông tin liên hệ: 0243.7368.315

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

- Phạm vi, quy mô của Hệ thống: Nhằm hỗ trợ công tác tổng hợp báo cáo, cung cấp số liệu đầy đủ, kịp thời và chính xác phục vụ hoạt động phòng chống bệnh không lây nhiễm. Quy mô của hệ thống cung cấp dịch vụ cho hơn 10.000 người sử dụng.

**4. Mô tả cấu trúc của hệ thống**

**4.1. Sơ đồ logic tổng thể**



Hình 1. Cấu trúc logic của Trung tâm dữ liệu

Các vùng mạng được thiết kế như sau:

Hệ thống mạng tại trung tâm dữ liệu y tế hiện nay bao gồm các phân hệ: Internet, DMZ, VPN, CORE, APP & DB, MGMT module.

- Phân hệ internet: bao gồm thiết bị định tuyến làm nhiệm vụ kết nối người dùng ra ngoài internet. Thiết bị firewall vừa làm nhiệm vụ bảo vệ vùng ngoài (internet) và vùng trong (internal).

- Phân hệ DMZ: bao gồm các ứng dụng, dịch vụ public ra ngoài internet.

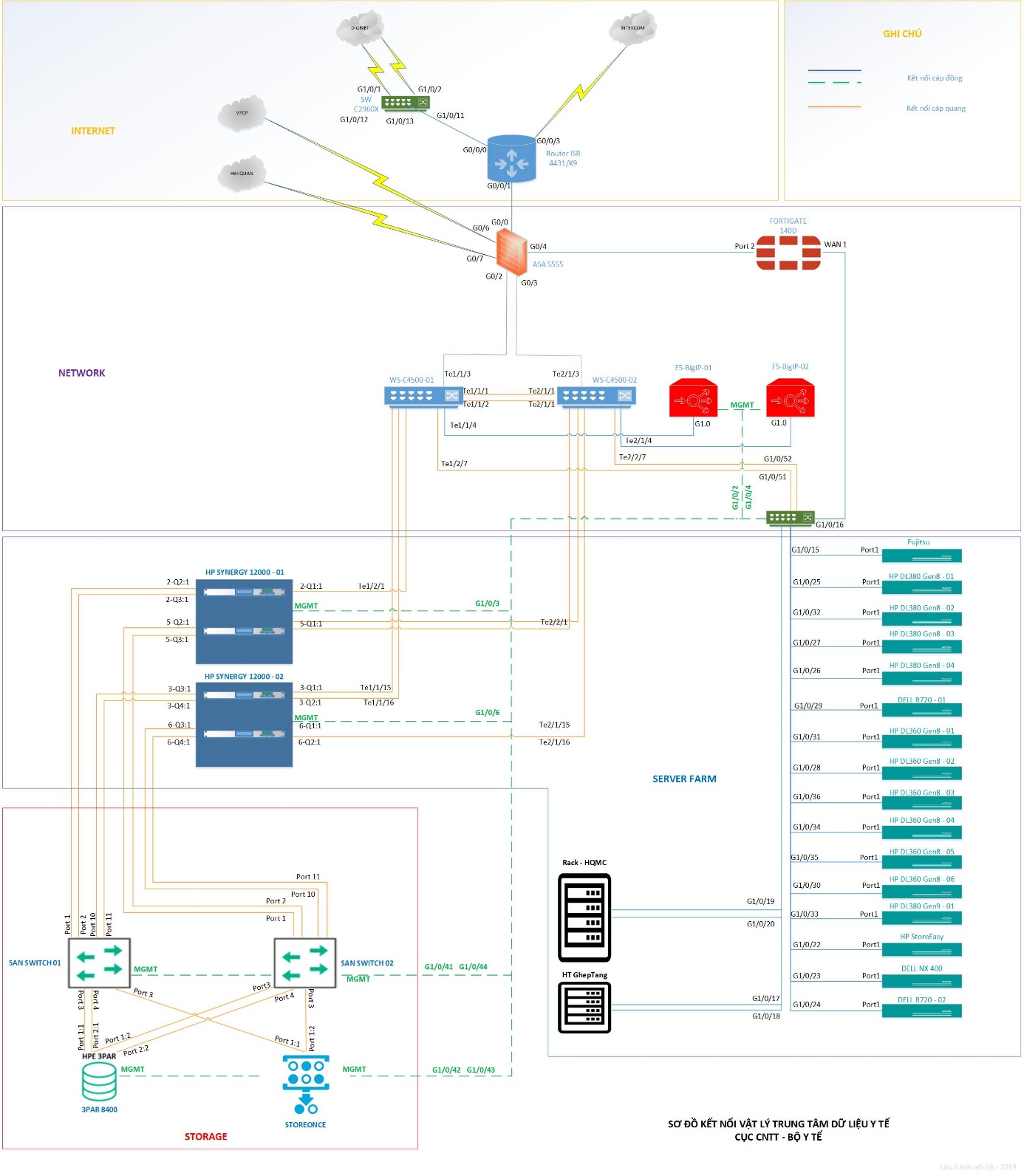
- Phân hệ VPN: gồm thiết bị fotigate làm nhiệm vụ tạo các kết nối VPN cho người dùng nghiệp vụ (người quản trị).

- Phân hệ Core: gồm cặp thiết bị chuyển mạch lõi, làm nhiệm vụ chuyển mạch tốc độ cao cho toàn hệ thống.

- Phân hệ APP và DB: bao gồm các máy chủ ứng dụng và máy chủ cơ sở dữ liệu của hệ thống.

- Phân vùng quản trị (MGMT): cung cấp các kết nối để quản trị toàn bộ phần hạ tầng (máy chủ, lưu trữ, sao lưu, tường lửa, chuyển mạch...).

**4.2. Sơ đồ 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** | **Số lượng** | **Mục đích sử dụng** |
| 1 | Router ISR 4431-K9 | 1 | Router biên |
| 2 | Chuyển mạch lõi WS C4500X-24X-IPB | 2 | Chuyển mạch lõi |
| 3 | FIREWALL ASA5555 | 1 | Tường lửa giữa vùng dmz và app, db |
| 4 | Web Application Firewall – WAF | 2 | Tường lửa ứng dụng Web |
| 5 | Thiết bị mạng WS-C2960X-48TS-L | 1 | Chuyển mạch access tới các máy chủ |
| 6 | SAN SWITCH HPE SN3000B 24-12 FC | 2 | Chuyển mạch hệ thống lưu trữ |
| 7 | F5-BIG-IP-LTM | 2 | Cân bằng tải dịch vụ |
| 8 | Cisco 2960 24 port | 2 | Thiết bị chuyển mạch cho các máy chủ cũ, dùng cổng 1Gbps đồng |
| 9 | Fortigate 140D | 1 | Dùng làm thiết bị VPN gateway cho người dùng quản trị các ứng dụng nghiệp vụ |
| 10 | Cisco ASA5525 | 1 | Dùng làm internet firewall/router cho hệ thống mạng LAN |
| 11 | Cisco catalyst 6807 | 1 | Dùng làm thiết bị chuyển mạch lõi cho hệ thống mạng LAN |
| 12 | Switch access tầng | 5 | Dùng làm thiết bị chuyển mạch truy cập cho người dùng tại các tầng. Các switch có nguồn gốc từ nhiều nhà cung cấp khác nhau. |
| 13 | Barracura | 2 | Thiết bị chặn lọc thư rác chuyên dụng |

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

**4.4. Danh mục các máy chủ, ứng dụng của hệ thống**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Máy chủ/Ứng dụng cài đăt/Vùng mạng/HĐH** | **Mục đích sử dụng** |
| 1 | **Hệ thống Phần mềm báo cáo bệnh không lây nhiễm.** | 1. **Máy chủ ứng dụng 01**   FrontEnd/BackEnd-APP01  IP:172.16.31.96  CPU: 16 vCPU  RAM: 16 GB  DISK: 200 GB   1. **Máy chủ ứng dụng 02**   FrontEnd/BackEnd-APP02  IP:172.16.31.97  CPU: 16 vCPU  RAM: 16 GB  DISK: 200 GB   1. **Máy chủ DB**   IP: 172.16.5.96  CPU: 16 vCPU  RAM: 16 GB  DISK: 500 GB | Hệ thống phần mềm báo cáo bệnh không lây nhiễm. |

Bảng 2. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Vùng mạng** | **IP Private** | **IP Public** |
| 1 | DMZ | 172.16.101.0/24  172.16.31.0/24  172.16.32.0/24 | 103.124.60.0/22 |
| 2 | Vùng mạng quản trị | 192.168.1.0/24 |  |
| 3 | Vùng máy chủ nội bộ | 172.16.2.0/24 |  |
| 4 | Vùng máy chủ APP, DB | 172.16.104.0/24  172.16.105.0/25  172.16.4.0/24  172.16.5.0/24 |  |

Bảng 3. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống

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

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hệ thống** | **Cấp độ đề xuất** | **Căn cứ đề xuất** |
| 1 | Hệ thống Phần mềm báo cáo bệnh không lây nhiễm (https://kln.tkyt.vn) | 3 | Khoản 2/Điều 9/NĐ85 |

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

***2.1. Hệ thống Phần mềm báo cáo bệnh không lây nhiễm***

Hệ thống phần mềm báo cáo bệnh không lây nhiễm phục vụ hoạt động của các cơ quan, tổ chức trong ngành Y tế. Căn cứ theo quy định tại Khoản 3/Điều 9/NĐ85, hệ thống này được đề xuất cấp độ 3.

***2.2. Sơ đồ tổng thể hệ thống***

Sơ đồ tổng thể hệ thống báo cáo bệnh không lây nhiễm

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Đơn vị thực hiện báo cáo** | | | | |
| Các cơ sở khám chữa bệnh. |  | - Bắt buộc đối với các CSYT đang được WHO hỗ trợ quản lý điều trị THA và ĐTĐ.  - Khuyến nghị các cơ sở KCB khác sử dụng. |  | Tất cả các cơ sở y tế. |

PHẦN MỀM THỐNG KÊ Y TẾ

API

API

PHẦN MỀM BÁO CÁO BỆNH KLN

HMIS

HIS

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Đầu ra** | | | | |
| Dữ liệu khám chữa bệnh |  | - Dữ liệu bệnh không lây nhiễm.  - Biểu mẫu báo cáo WHO |  | - Biểu mẫu báo cáo tổng hợp theo Thông tư 73.  - Biểu mẫu báo cáo tổng hợp theo CV277 |

**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

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.

Thuyết minh phương án bảo đảm an toàn thông tin về kỹ thuật liên quan đến việc thiết kế, thiết lập cấu hình hệ thống và liên quan trực tiếp đến đầu tư. Do ở TT Dữ liệu – Cục Công nghệ thông tin – Bộ Y tế sử dụng chung hạ tầng, thiết bị hệ thống. Vì vậy, thuyết minh phương án đáp ứng yêu cầu kỹ thuật được thuyết minh chung tại Phụ lục II.

Hiện tại ở trung tâm dữ liệu của Trung tâm dữ liệu y tế – Cục Công nghệ thông tin – Bộ Y tế tất cả các hệ thống đều được sử dụng chung các hạ tầng, thiết bị hệ thống… Vì vậy phương án bảo đảm an toàn thông tin cho Hệ thống thông tin của Bộ Y tế sẽ được thuyết minh ở cấp độ cao nhất là cấp độ 3.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hệ thống** | **Cấp độ đề xuất** | **Nội dung thuyết minh** |
| 1 | Thuyết minh phương án đáp ứng yêu cầu quản lý | 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**

**1. Thiết lập chính sách an toàn thông tin**

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

|  |  |
| --- | --- |
| **Yêu cầu** | Xác định các mục tiêu, nguyên tắc bảo đảm an toàn thông tin |
| **Mô tả khả năng đáp ứng** | Đáp ứng. Cụ thể:  Đã có quy chế về các chính sách đảm bảo an toàn thông tin. |
| **Yêu cầu** | 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 |
| **Mô tả khả năng đáp ứng** | Đáp ứng. Cụ thể: |

***1.2. Xây dựng và công bố***

|  |  |
| --- | --- |
| **Yêu cầu** | Quy định về xây dựng và công bố Quy chế bảo đảm an toàn thông tin |
| **Mô tả khả năng đáp ứng** | Đáp ứng. Cụ thể: |

***1.3. Rà soát, sửa đổi***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin |
| **Mô tả khả năng đáp ứng** | Đáp ứng. Cụ thể: |

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

***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 |
| **Mô tả khả năng đáp ứng** | Đáp ứng, cụ thể: Phòng Y tế điện tử chỉ đạo công tác bảo đảm ATTT |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc phối hợp với những cơ quan/tổ chức có thẩm quyền |
| **Mô tả khả năng đáp ứng** | Đáp ứng. Cụ thể:  Theo quy định tại điều 2, Quyết định 6126/QĐ-BYT ngày 10 tháng 10 năm 2018. |

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

***3.1. Tuyển dụng***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ |
| **Mô tả khả năng đáp ứng** | Đáp ứng. Cụ thể:  Theo quy định tại điều 2, Quyết định 6126/QĐ-BYT ngày 10 tháng 10 năm 2018. |

***3.2. Trong quá trình làm việc***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc |
| **Mô tả khả năng đáp ứng** | 1. Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống  a) Với người sử dụng:  Đáp ứng. Cụ thể:  b) Với cán bộ quản lý và vận hành hệ thống  Đáp ứng. Cụ thể:  2. Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về ATTT cho người sử dụng.  Đáp ứng. Cụ thể:  3. Định kỳ hàng năm, tổ chức đào tạo các kỹ năng cơ bản về ATTT cho người sử dụng.  Đáp ứng. Cụ thể:  Định kỳ hàng năm đơn vị có người sử dụng được tổ chức đào tạo các kỹ năng cơ bản về an toàn thông tin theo chương trình, nội dung tại - Quyết định số 99/QĐ-TTg ngày 14/01/2014 phê duyệt Đề án Đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc |
| **Mô tả khả năng đáp ứng** | * Đáp ứng. Cụ thể: Có quy định về nghỉ việc, chuyển việc đối với nhân viên. |

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

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về thiết kế an toàn hệ thống thông tin |
| **Mô tả khả năng đáp ứng** | Đáp ứng. Cụ thể: Hệ thống mạng tại Trung tâm Dữ liệu y tế được phê duyệt trước khi đưa vào triển khai |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về phát triển phần mềm thuê khoán |
| **Phương án** | Chưa đáp ứng. Cụ thể: Sẽ hoàn thiện trước 31/21/2021 |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc thử nghiệm và nghiệm thu hệ thống |
| **Phương án** | Đáp ứng. Cụ thể: Theo quy định của pháp luật về nghiệm thu |

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

***5.1. Quản lý an toàn mạng***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý an toàn mạng |
| **Phương án** | Đáp ứng. Cụ thể:  - Đơn vị có quy trình cụ thể về quản lý an toàn mạng.  - Đơn vị thực hiện việc giám sát dựa trên các giải pháp kỹ thuật: tưởng lửa, IPS, hệ thống giám sát mạng Nagios, hệ thống bảo vệ website WAF Inperva , giải pháp dò quét lỗ hổng ứng dụng web, ... |

***5.2. Quản lý an toàn máy chủ và ứng dụng***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý an toàn máy chủ và ứng dụng |
| **Phương án** | Đáp ứng. Cụ thể: Đơn vị có quy trình cụ thể về quản lý an toàn máy chủ và ứng dụng |

***5.3. Quản lý an toàn dữ liệu***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý an toàn dữ liệu |
| **Phương án** | Đáp ứng. Cụ thể: Có quy định về quản lý an toàn dữ liệu |

***5.4. Quản lý an toàn thiết bị đầu cuối***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý thiết bị đầu cuối |
| **Phương án** | Đáp ứng. Cụ thể: Có quy định về quản lý thiết bị đầu cuối |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý phòng chống phần mềm độc hại |
| **Phương án** | Đáp ứng. Cụ thể: Có quy định về quản lý phòng chống phần mềm độc hại |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý giám sát an toàn hệ thống thông tin |
| **Phương án** | Đáp ứng. Cụ thể: Có quy định về quản lý giám sát an toàn hệ thống thông tin |

***5.7. Quản lý điểm yếu an toàn thông tin***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý điểm yếu an toàn thông tin |
| **Phương án** | Đáp ứng. Cụ thể: Có quy định về quản lý điểm yếu an toàn thông tin |

***5.8. Quản lý sự cố an toàn thông tin***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý sự cố an toàn thông tin |
| **Phương án** | Đáp ứng. Cụ thể: Có quy định về quản lý sự cố an toàn thông tin |

***5.9. Quản lý an toàn người sử dụng đầu cuối***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý an toàn người sử dụng đầu cuối |
| **Phương án** | Đáp ứng. Cụ thể: Có quy định về quản lý an toàn người sử dụng đầu cuối |

**PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN ĐÁP ỨNG YÊU CẦU KỸ THUẬT**

Hệ thống Chứng nhận tiêm Vắc xin Covid-19 điện tử được đặt tại trung tâm dữ liệu y tế - Cục Công nghệ thông tin – Bộ Y tế được xác định ở cấp độ 3 theo khoản 2/Điều 9/NĐ85. Hệ thống được sử dụng chung với các hệ thống thành phần khác trong hệ thống như hạ tầng mạng, hệ thống lưu trữ, tường lửa… Vì vậy sẽ thuyết minh hệ thống thông tin theo 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 | Có | Đáp ứng.  Cụ thể: Vùng mạng nội bộ độc tập, tách riêng khỏi hệ thống của trung tâm dữ liệu |
| 2 | Vùng mạng biên | Có | Đáp ứng.  Cụ thể: Kết nối hệ thống với mạng Internet và mạng diện rộng và cả mạng nội bộ của cơ quan. |
| 3 | Vùng DMZ | Có | Đáp ứng.  Cụ thể: Vùng DMZ kêt nối mạng Internet và mạng diện rộng, cả mạng nội bộ của cơ quan. |
| 4 | Vùng máy chủ nội bộ | Có | Đáp ứng.  Cụ thể: Vùng máy chủ nội bộ, cung cấp các dịch vụ nội bộ |
| 5 | Vùng mạng máy chủ cơ sở dữ liệu | Có | - Đáp ứng.  - Cụ thể: Lưu trữ và quản lý cơ sở dữ liệu tập trung của các hệ thống thành phần |
| 6 | Vùng mạng không dây | Có | - Đáp ứng.  - Cụ thể: Vùng mạng không dây được sử dụng cho người dùng tại cơ quan, độc lập không kết nối tới được tới vùng mạng của máy chủ. |
| 7 | Vùng quản trị | Có | - Đáp ứng.  - Cụ thể: Có vùng mạng riêng dành cho quản trị. |

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 | - Đáp ứng.  - Cụ thể: Các thiết bị hệ thống/máy chủ được thiết lập cấu hình cho phép quản trị từ xa an toàn thông qua VPN. |
| 2 | Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập | Có | - Đáp ứng.  - Cụ thể: Truy cập giữa các vùng mạng được quản lý và phòng chống xâm nhập sử dụng các thiết bị tường lửa chuyên dụng có tích hợp chức năng phòng chống xâm nhập. |
| 3 | Phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính | Có | - Đáp ứng một phần  - Cụ thể: Hiện tại Trung tâm dữ liệu y tế chưa có các thiết bị dự phòng nóng cho các thiết bị thiết bị tường lửa lõi và Router biên. |
| 4 | Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu | Có | - Đáp ứng.  - Cụ thể: Đã có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu. |
| 5 | Phương án chặn lọc phần mềm độc hại trên môi trường mạng | Có | - Đáp ứng.  - Cụ thể: Trung tâm dữ liệu đã triển khai hệ thống WAF-Inperva và thiết bị chặn lọc thư rác chuyên dụng Imperva |
| 6 | Phương án phòng chống tấn công từ chối dịch vụ | Có | - Đáp ứng.  - Cụ thể: Trung tâm dữ liệu đã triển khai hệ thống WAF-Inperva và firewall ASA 555 để phòng chống, phát hiện, giảm thiểu rủi ro tấn công từ chối dịch vụ và yêu cầu đơn vị cung cấp đường truyền ISP hỗ trợ khi hệ thống mạng tại Trung tâm Dữ liệu bị tấn công DDoS |
| 7 | Phương án giám sát hệ thống thông tin tập trung | Có | - Đáp ứng.  - Cụ thể: Hiện tại trung tâm đang sử dụng hệ thống Nagios, Cati để giám sát hệ thống thông tin tập trung. |
| 8 | Phương án giám sát an toàn hệ thống thông tin tập trung | Có | - Đáp ứng  - Cụ thể: Hệ thống đang sử dụng splunk để giám sát an toàn hệ thống. |
| 9 | Phương án quản lý sao lưu dự phòng tập trung | Có | - Đáp ứng.  - Cụ thể: Sử dụng hệ thống HP StoreOne của hãng HP, có năng lực quản lý và lưu trữ 80TB dữ liệu. |
| 10 | Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung | Có | * Đáp ứng. * Cụ thể: Các hệ thống thông tin và máy tính người dùng tại Cục CNTT đã được cài đặt phần mềm antivirus Kaspersky tập trung. |
| 11 | Có phương án phòng, chống thất thoát dữ liệu | Chưa có | * Chưa đáp ứng. * Cụ thể: Chưa có phương án phòng, chống thất thoát dữ liệu. Sẽ bổ phương án và giải pháp (Thực hiện trước 12/2021). |
| 12 | Có phương án dự phòng kết nối mạng Internet cho hệ thống | Có | * Đáp ứng * Cụ thể: Sử dụng đồng thời hai kết nối Internet của hai nhà cung cấp dịch vụ khác nhau. |

***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 | * Đáp ứng. * Cụ thể: Hệ thống được thiết lập chỉ cho phép kết nối mạng có hỗ trợ mã hóa, xác thực khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet. |
| 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 | * Đáp ứng * Cụ thể: Hiện tại trung tâm dữ liệu có thiết bị F5 để kiểm soát truy cập, ngăn chặn từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể. |
| 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 | * Đáp ứng. * Cụ thể: Trên thiết bị ASA thiết lập thời gian chờ là 8 tiếng. |
| 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 | * Đáp ứng. * Cụ thể: 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 | * Đáp ứng. * Cụ thể: 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 FW01-08. |

***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 | * Đáp ứng * Cụ thể: Truy cập máy chủ qua VPN và theo thời gian đăng kí vào máy chủ đăng kí |
| 2 | Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian | Có | * Chưa đáp ứng * Cụ thể: Truy cập máy chủ qua VPN và theo thời gian đăng kí vào máy chủ đăng kí |
| 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 | Có | * Đáp ứng. * Cụ thể: Vùng mạng nội bộ và vùng mạng hệ thống ở TT Dữ liệu y tế là hai vùng mạng độc lập, để truy cập được vào vùng mạng hệ thống cần phải sử dụng VPN để truy cập. |

***1.4. Nhật ký hệ thống***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có lưu trữ nhật ký các thiết bị mạng và quản lý tập trung trong vùng mạng quản trị đối với các thiết bị mạng có hỗ trợ tính năng này hoặc thiết bị mạng quan trọng; | Có | * Đáp ứng. * Cụ thể: Các thiết bị mạng có hỗ trợ tính năng và các thiết bị mạng quan trọng đều được lưu trữ nhật ký |
| 2 | Có lưu trữ tối thiểu trong 03 tháng đối với nhật ký của các thiết bị mạng và bảo đảm động bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam | Có | * Đáp ứng. * Cụ thể: Khi cấu hình thiết bị |
| 3 | Có ghi nhật ký đối với các hoạt động trên thiết bị mạng nội bộ và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian; | Có | * Đáp ứng. * Cụ thể: Cấu hình thiết bị |

***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 | Chưa có | * Chưa đáp ứng. * Cụ thể: |
| 2 | Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng | Chưa  Có | * Đáp ứng. * Cụ thể: WAF |
| 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 | * Đáp ứng. * Cụ thể: WAF |

***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 | * Đáp ứng. * Cụ thể: WAF, Barracura |
| 2 | Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại | Có | * Chưa đáp ứng. * Cụ thể: WAF, Barracura |
| 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 | * Chưa đáp ứng. * Cụ thể: WAF, Barracura |

***1.7. Bảo vệ thiết bị hệ thống***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Cấu hình chức năng xác thực trên các thiết bị | Có | * Đáp ứng. * Cụ thể: Các thiết bị đều cấu hình mặc định xác thực bằng cơ chế mật khẩu bảo đảm độ phức tạp cần thiết và tự động yêu cầu thay đổi mật khẩu định kỳ theo quy định. |
| 2 | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa | Có | * Đáp ứng. * Cụ thể: Để truy cập, quản trị các thiết bị từ xa cần phải sử dụng VPN để truy cập. |
| 3 | Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa | Có | * Đáp ứng. * Cụ thể: Để quản trị các thiết bị từ xa, người quản trị cần phải sử dụng VPN để truy cập. |
| 4 | Hạn chế được số lần đăng nhập sai | Có | * Đáp ứng. * Cụ thể: Đã thiết lập cấu hình hạn chế số lần đăng nhập sai vào thiết bị. |
| 5 | Phân quyền truy cập, quản trị thiết bị | Có | * Đáp ứng. * Cụ thể: Tại trung tâm dữ liệu các thiết bị bảo vệ hệ thống được phần quyền truy cập cho từng người quản trị đúng theo quyền hạn của từng người quản trị. |
| 6 | Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng | Có | * Đáp ứng. * Cụ thể: Trước khi đứa vào sử dụng trung tâm dữ liệu có tiến hành kiểm tra, xử lý điểm yếu an toàn thông tin của thiết bị trước khi đưa vào sử dụng. |

**2. Bảo đảm an toàn máy chủ**

***2.1. Xác thực***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Thiết lập chính sách xác thực trên máy chủ | Có | * Đáp ứng. * Cụ thể: Các máy chủ trong hệ thống thông tin đã cấu hình mặc định xác thực bằng cơ chế mật khẩu. |
| 2 | Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa | Có | * Chưa đáp ứng. * Cụ thể: Rà soát các tài khoản trên máy chủ |
| 3 | Thiết lập chính sách mật khẩu an toàn. | Có | * Đáp ứng * Cụ thể: Theo quy trình vận hành phòng máy chủ đã có chính sách thiết lập mật khẩu an toàn. |
| 4 | Hạn chế số lần đăng nhập sai. | Có | * Đáp ứng một phần * Cụ thể: Chưa có chính sách hạn chế số lần đăng nhập sai trên máy chủ trên tất cả các máy chủ. |
| 5 | Vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định. | Chưa có | * Chưa đáp ứng * Cụ thể: Chưa có chính sách hạn chế số lần đăng nhập sai trên máy chủ. |

***2.2. Kiểm soát truy cập***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa | Có | * Đáp ứng. * Cụ thể: Các máy chủ trong hệ thống thông tin đã cấu hình mặc định để tất cả kết nối được mã hóa trong việc quản trị máy chủ từ xa. |
| 2 | Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi máy chủ không nhận được yêu cầu từ người dùng; | Có | * Đáp ứng. * Cụ thể: Thời gian chờ trên VPN được thiết lập là 8 giờ. |
| 3 | Thay đổi cổng quản trị mặc định của máy chủ; | Có | * Đáp ứng một phần * Cụ thể: Một số máy chủ ở trung tâm dữ liệu vẫn sử dụng cổng quản trị mặc định |
| 4 | Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa | Có | * Chưa đáp ứng * Cụ thể: Truy cập qua tài khoản VPN |

***2.3. Nhật ký hệ thống máy chủ***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ | Có | * Đáp ứng. * Cụ thể: Các máy chủ đã được thiết lập chức năng ghi nhật ký hệ thống trên các máy chủ. |
| 2 | Đồng bộ thời gian giữa máy chủ với máy chủ thời gian | Có | * Chưa đáp ứng * Cụ thể: Tại trung tâm dữ liệu có máy chủ thời gian. |
| 3 | Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống | Có | * Chưa đáp ứng * Cụ thể: Các máy chủ đã được thiết lập chính sách này. |
| 4 | Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ | Chưa có | * Chưa đáp ứng * Cụ thể: Hiện tại trung tâm dữ liệu chưa có hệ thống lưu trữ nhật ký tập trung. |
| 5 | Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng | Có | * Đáp ứng một phần * Cụ thể: Hiện tại trung tâm dữ liệu chưa có hệ thống lưu trữ nhật ký tập trung, chủ yếu log hệ thống sẽ lưu trữ trên máy chủ dịch vụ, thiết bị mang, bảo mật |

***2.4. Phòng chống xâm nhập***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ | Có | * Chưa đáp ứng. * Cụ thể: Cơ bản các máy chủ đã được loại bỏ các tài khoản không sử dụng. |
| 2 | Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ | Có | * Đáp ứng * Cụ thể: Tất cả các máy chủ đều được bật tường lừa của hệ điều hành để cấm các truy cập trái phép tới máy chủ. |
| 3 | Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng | Có | * Đáp ứng * Cụ thể: Các giao thức mạng không an toàn và dịch vụ hệ thống không sử dụng đều bị vô hiểu hóa. |
| 4 | Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. | Có | * Chưa đáp ứng * Cụ thể: Yêu cầu các hệ thống đánh giá an toàn thông tin, cập nhật hệ điều hành, cài đặt phần mềm AV trước khi đưa vào sử dụng |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật | Có | * Đáp ứng * Cụ thể: Trên các máy chủ đặt tại trung tâm dữ liệu đã được cài đặt phần mềm antivirus Kaspersky. |
| 2 | Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt | Có | * Đáp ứng * Cụ thể: Các phần mềm trước khi cài đặt lên máy chủ đều được kiểm tra, dò quét trước khi cài đặt |
| 3 | Quản lý tập trung các phần mềm phòng chống mã độc cài đặt trên máy chủ | Có | * Đáp ứng * Cụ thể: Hiện trung tâm dữ liệu đang sử dụng phần mềm antivirus Kaspersky quản lý tập trung. |

***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 | * Đáp ứng * Cụ thể: Tất cả máy chủ tại trung tâm dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng đều được làm sạch. |
| 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 | Chưa  Có | * Chưa đáp ứng * Cụ thể: Trung tâm dữ liệu đã thực hiện sao lưu dự phòng thông tin, dữ liệu trên máy chủ trước khi xóa. |
| 3 | Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa | ChưaCó | * Chưa đáp ứng * Cụ thể: Hiện tại trung tâm dữ liệu chưa có biện pháp kiểm tra bảo đảm dữ liệu không thể khôi phục sau khi xóa. * Quy định trước 31/12/2021 |

**3. Bảo đảm an toàn ứng dụng**

***3.1. Xác thực***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng | Chưa  Có | * Chưa đáp ứng * Cụ thể: Trung tâm dữ liệu chưa có phương án để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng. |
| 2 | Lưu trữ có mã hóa thông tin xác thực hệ thống | Có | * Đáp ứng * Cụ thể: Các thông tin xác thực đều được lưu dưới dạng mã hóa. |
| 3 | Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng | Có | * Đáp ứng * Cụ thể: Các ứng dụng trong hệ thống thông tin đã cấu hình mặc định xác thực bằng cơ chế mật khẩu bảo đảm độ phức tạp cần thiết và tự động yêu cầu thay đổi mật khẩu định kỳ theo quy định. |
| 4 | Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định | Có | * Đáp ứng * Cụ thể: Mốt số úng dụng quan trọng cho người sử dụng đã được cầu hình hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định. * Ví dụ như: Hệ thống thư điện tử.. |
| 5 | Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng. | Có | * Đáp ứng * Cụ thể: Hầu hết các ứng dụng tại trung tâm dữ liệu đã được cài đặt SSL để mã hóa thông tin. |
| 6 | Thiết lập cấu hình ứng dụng để ngăn cản việc đăng nhập tự động đối với các ứng dụng | Chưa có | * Chưa đáp ứng * Cụ thể: Các ứng dụng chưa được cầu hình để ngăn cản việc đăng nhập tự động. |

***3.2. Kiểm soát truy cập***

***3.3. Nhật ký hệ thống***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | 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 | Có | * Đáp ứng * Cụ thể: Các ứng dụng đều lưu lại nhật ký hệ thống. |
| 2 | Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung | Chưa  Có | * Chưa đáp ứng * Cụ thể: Chưa có hệ thống quản lý và lưu trữ nhật ký hệ thống tập trung. |
| 3 | Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng | Có | * Đáp ứng * Cụ thể: Nhật ký hệ thống đều đươc lưu trữ trong khoảng 03 tháng. |

***3.4. Bảo mật thông tin liên lạc***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | 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. | Có | * Đáp ứng * Cụ thể: Theo quy định nhà nước |
| 2 | 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 | Có | * Chưa đáp ứng * Cụ thể: VPN |

***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 | + |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý | Có | - Đáp ứng  - Cụ thể: Hiện tại trên hạ tầng thông tin đã sử dụng hệ thống WAF Inperva để kiểm tra, chặn lọc những thuộc tính không hợp lệ. |
| 2 | Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu | Có | - Đáp ứng  - Cụ thể: Hiện tại trên hạ tầng thông tin đã sử dụng hệ thống WAF Inperva để kiểm tra, chặn lọc những thuộc tính không hợp lệ. |
| 3 | Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa | Có | * Đáp ứng. * Cụ thể: Để truy cập vào các trang quản trị ứng dụng từ xa người quản trị phải sử dụng VPN để truy cập. |
| 4 | 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 | Có | * Đáp ứng. * Cụ thể: Hiện tại trên hạ tầng thông tin đã sử dụng hệ thống WAF Inperva để bảo vệ các ứng dụng chống lại các cuộc tấn công như SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF. |

**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 | * Đáp ứng. * Cụ thể: Tại trung tâm dữ liệu có thiết bị HP Store One để lưu trữ dữ liệu. |

***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 | Chưa  Có | * Chưa đáp ứng. * Cụ thể: Chưa có phần mềm/thực hiện giải pháp hỗ trợ lưu trữ mã hóa. |

***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 | * Đáp ứng. * Cụ thể: Tại trung tâm dữ liệu có thiết bị HP Store One để lưu trữ dữ liệu. |
| 2 | Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau | Có | * Đáp ứng. * 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 | * Đáp ứng. * Cụ thể: Tại trung tâm dữ liệu có thiết bị HP Store One để lưu trữ dữ liệu và được phân vung riêng biệt để sao lưu dự phòng. |