|  |
| --- |
| **(CHỦ QUẢN HỆ THỐNG THÔNG TIN)****(ĐƠN VỊ VẬN HÀNH)****HỒ SƠ MẪU****HỒ SƠ ĐỀ XUẤT CẤP ĐỘ 1****(TÊN HỆ THỐNG THÔNG TIN)****Tỉnh A – 20xx** |

**MỤC LỤC**

[THUẬT NGỮ, TỪ VIẾT TẮT 1](#_Toc116482074)

[DANH MỤC CÁC BẢNG 2](#_Toc116482075)

[DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ 3](#_Toc116482076)

[PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN 4](#_Toc116482077)

[1. Thông tin Chủ quản hệ thống thông tin 4](#_Toc116482078)

[2. Thông tin Đơn vị vận hành 4](#_Toc116482079)

[3. Mô tả phạm vi, quy mô của hệ thống 4](#_Toc116482080)

[4. Mô tả cấu trúc của hệ thống 4](#_Toc116482081)

[**4.1. Mô hình logic tổng thể** 4](#_Toc116482082)

[**4.2. Mô hình kết nối vật lý** 6](#_Toc116482083)

[**4.3. Danh mục thiết bị sử dụng trong hệ thống** 6](#_Toc116482084)

[**4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống** 7](#_Toc116482085)

[**4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống** 7](#_Toc116482086)

[PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT 8](#_Toc116482087)

[1. Danh mục hệ thống thông tin và cấp độ đề xuất 8](#_Toc116482088)

[2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin 8](#_Toc116482089)

[PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM 9](#_Toc116482090)

[AN TOÀN HỆ THỐNG THÔNG TIN 9](#_Toc116482091)

[PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 1 11](#_Toc116482092)

[**5.1.1. Thiết lập chính sách an toàn thông tin** 11](#_Toc116482093)

[**5.1.2. Tổ chức bảo đảm an toàn thông tin** 14](#_Toc116482094)

[**5.1.3. Bảo đảm nguồn nhân lực** 15](#_Toc116482095)

[**5.1.4. Quản lý thiết kế, xây dựng hệ thống thông tin** 17](#_Toc116482096)

[**5.1.5. Quản lý vận hành hệ thống thông tin** 18](#_Toc116482097)

[**5.1.6. Phương án Quản lý rủi ro an toàn thông tin** 20](#_Toc116482098)

[**5.1.7. Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin** 21](#_Toc116482099)

[PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG CẤP ĐỘ 1 23](#_Toc116482100)

[**5.2.1. Bảo đảm an toàn mạng** 23](#_Toc116482101)

[**5.2.2. Bảo đảm an toàn máy chủ** 26](#_Toc116482102)

[**5.2.3. Bảo đảm an toàn ứng dụng** 27](#_Toc116482103)

[**5.2.4. Bảo đảm an toàn dữ liệu** 28](#_Toc116482104)

# THUẬT NGỮ, TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **Từ viết tắt** | **Nghĩa đầy đủ** |
|  | CNTT | Công nghệ thông tin |
|  | CSDL | Cơ sở dữ liệu |
|  | LAN | Mạng nội bộ |
|  | VPN | Vitural Private Network |
|  | DNS  | Domain Name Server |

**DANH MỤC CÁC BẢNG**

[Bảng 1. Danh mục thiết bị sử dụng trong hệ thống 6](#_Toc67302049)

[Bảng 2. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống 7](#_Toc67302050)

[Bảng 3. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống 7](#_Toc67302051)

**DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ**

[Hình 1. Cấu trúc logic của hệ thống 5](#_Toc67302056)

[Hình 2. Kết nối vật lý của hệ thống 6](#_Toc67302057)

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

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

**- Tên tổ chức: UBND huyện / thành phố / thị xã**

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

- Người đại diện: Ông Trần Văn A, Chức vụ: Chủ tịch UBND huyện / thành phố / thị xã.

- Địa chỉ: Địa chỉ trụ sở của đơn vị.

- Thông tin liên hệ: Số điện thoại, Thư điện tử.

**2. Thông tin dơn vị vận hành**

**- Tên dơn vị vận hành: UBND các xã / phường / thị trấn.**

- Người đại diện: Chủ tịch UBND **các xã / phường / thị trấn**

- Địa chỉ: Địa chỉ của UBND **các xã / phường / thị trấn**.

- Thông tin liên hệ: Số điện thoại, Thư điện tử.

(Có phụ lục danh sách kèm theo)

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

- Phạm vi, quy mô của Hệ thống mạng LAN: Hệ thống thông tin của UBND các xã / phường / thị trấn được thiết lập để phục vụ công tác chỉ đạo điều hành và cung cấp dịch vụ trong phạm vi nội bộ đơn vị.

- Đối tượng phục vụ của hệ thống: Cán bộ, công chức, viên chức, người lao động của UBND các xã / phường / thị trấn và người dân đến làm việc với đơn vị.

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

+ Hệ thống mạng LAN.

**4. Mô tả cấu trúc của hệ thống**

**4.1. Mô hình logic tổng thể**



Hình 1. Cấu trúc logic của hệ thống

Các vùng mạng được thiết kế như sau:

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

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

**4.2. Mô hình kết nối vật lý**

**4.2.1. Mô hình kết nối vật lý**

****

Hình 2. Kết nối vật lý của hệ thống

**4.2.2 Mô hình kết nối vật lý cụ thể**

Mô hình kết nối vật lý hệ thống mạng LAN của UBND các xã, phường, thị trấn tại phụ lục kèm theo.

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

Danh mục thiết bị sử dụng trong hệ thống mạng LAN của UBND các xã, phường, thị trấn tại phụ lục kèm theo.

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

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên dịch vụ** | **Mục đích sử dụng** |
| 1 | Kết nối mạng | Cung cấp kết nối cục bộ (LAN) giữa các thiết bị máy tính làm việc của cán bộ, công chức, viên chức, người lao động trong đơn vị. |
| 2 | Kết nối mạng | Cung cấp kết nối internet, kết nối đến mạng SLCD cho máy tính làm việc của cán bộ, công chức, viên chức, người lao động trong đơn vị. |
| 3 | Kết nối mạng | Cung cấp kết nối internet cho khách, người dân đến làm việc tại đơn vị |

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** | **Đơn vị** | **Vùng mạng biên** | Vùng mạng nội bộ | Vùng mạng Publish / Guest |
| 1 | Xã a | 202.191.z.0/24 | 192.168.3.0/24 | 192.168.22.xxx/24 |
| 2 | Xã b | 202.191.z.0/24 | 192.168.4.0/24 | 192.168.22.xxx/24 |
| 3 | Xã … |  |  |  |

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

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

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

Hệ thống thông tin của tỉnh A bao gồm hệ thống thành phần với cấp độ đề xuất tương ứng, bao gồm:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hệ thống**  | **Cấp độ đề xuất** | **Căn cứ đề xuất** |
| 1 | Hệ thống Mạng LAN | 1 | Điều 7/NĐ85 |

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

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

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

**AN TOÀN HỆ THỐNG THÔNG TIN**

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

1. Thiết lập chính sách an toàn thông tin

2. Tổ chức bảo đảm an toàn thông tin

3. Bảo đảm nguồn nhân lực

4. Quản lý thiết kế, xây dựng hệ thống

5. Quản lý vận hành hệ thống

- Quản lý an toàn mạng

- Quản lý an toàn máy chủ và ứng dụng

- Quản lý an toàn dữ liệu

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. Nhật ký hệ thống

1.4. Phòng chống xâm nhập

1.5. Bảo vệ thiết bị hệ thống

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

2.2. Kiểm soát truy cập

2.3. Nhật ký hệ thống

2.4. Phòng chống xâm nhập

2.5. Phòng chống phần mềm độc hại

3. Bảo đảm an toàn ứng dụng

3.1. Xác thực

3.2. Kiểm soát truy cập

3.3. Nhật ký hệ thống

4. Bảo đảm an toàn dữ liệu

4.1. Sao lưu dự phòng

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

Thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống của tỉnh A sẽ bao gồm các thuyết minh thành phần sau:

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

**PHỤ LỤC I. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ VỚI CẤP ĐỘ 1**

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

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

|  |  |
| --- | --- |
| **Yêu cầu** | Xây dựng chính sách, quy trình quản lý, vận hành hoạt động bình thường của hệ thống nhằm bảo đảm tính sẵn sàng của hệ thống trong quá trình vận hành, khai thác. |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 9. Quản lý an toàn mạng***1. Quản lý, vận hành và bảo đảm an toàn hệ thống mạnga) Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.b) Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng. c) Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.2. Truy cập và quản lý cấu hình hệ thốnga) Cán bộ quản lý truy cập, khai thác thông tin 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 có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, 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.***Điều 10. 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) Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị.b) Các hệ thống thông tin cần có phướng án giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. c) 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.d) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.- Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.- Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.- 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 chủBảo 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 dụnga) 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 cốTriển 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.5. Cài đặt, gỡ bỏ hệ điều hành, dịch vụ, phần mềm trên hệ thống máy chủ và ứng dụng:Bộ phận chuyên trách về công nghệ thông tin của đơn vị chịu trách nhiệm cài đặt phần mềm cho máy tính phục vụ công việc. Người dùng không được can thiệp vào các phần mềm đã cài đặt trên máy tính (thay đổi, gỡ bỏ…) khi chưa được sự đồng ý của bộ phận công nghệ thông tin của đơn vị.6. Kết nối và gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thốnga) Cấu hình tối ưu và tăng cường bảo mật (cứng hóa) cho hệ thống máy chủ trước khi đưa vào vận hành, khai thác.b) Trước khi gỡ bỏ hệ thống máy chủ và dịch vụ khỏi hệ thống: Phải sao lưu dữ liệu trước khi gỡ bỏ. Phải xoá dữ liệu, ghi đè dữ liệu, format ổ cứng trên thiết bị. Một số trường hợp đặc biệt có thể cần phải phá huỷ vật lý thiết bị/vật lưu trữ trước khi bỏ đi.7. Các máy chủ trước khi đưa vào vận hành khai thác cần triển khai một số yêu cầu tối ưu và tăng cường bảo mật (cứng hóa) như:a) Sử dụng hệ điều hành bảo đảm an toàn thông tin.b) Loại bỏ hoặc tắt tất cả các dịch vụ không cần thiết.c) Sử dụng các phiên bản phần mềm an toàn.d) Kiểm soát truy cập và ghi nhận lại hoạt động (log) của tất cả các dịch vụ.đ) Cấm tất cả các truy cập từ bên ngoài vào hệ thống, chỉ cấp quyền truy cập xác đáng cho các người dùng tin cậy.e) Kiểm soát truy cập ở cấp người dùng cho mỗi dịch vụ.***Điều 11. Quản lý an toàn dữ liệu***1. Yêu cầu an toàn đối với phương pháp mã hóaa) 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. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ:a) Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.b) Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang/cổng thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho các tổ chức, cá nhân bên ngoài.c) Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.5. Sao lưu dự phòng và khôi phục dữ liệu:a) Lập danh sách các dữ liệu, phần mềm cần được sao lưu, có phân loại theo thời gian lưu trữ, thời gian sao lưu, phương pháp sao lưu và thời gian kiểm tra phục hồi hệ thống từ dữ liệu sao lưu.b) Xây dựng tài liệu, quy trình hướng dẫn sao lưu/phục hồi dữ liệu của hệ thống: Đơn vị quản trị hệ thống thực hiện xây dựng Tài liệu hướng dẫn sao lưu cụ thể đối với từng hệ thống cung cấp dịch vụ, hệ thống điều hành mà đơn vị quản lý.6. Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ:a) Định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên hệ thống (nếu có).b) Thực hiện sao lưu dữ liệu định kỳ: Cán bộ phụ trách sao lưu thực hiện sao lưu định kỳ theo phương án sao lưu đã được phê duyệt.c) Kiểm tra định kỳ: Dữ liệu sao lưu phải được lưu trữ an toàn và được kiểm tra thường xuyên đảm bảo sẵn sàng cho việc sử dụng khi cần. Kiểm tra, phục hồi hệ thống từ dữ liệu sao lưu.***Điều 17. 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) Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP).b) 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.c) 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.d) 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.đ) Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.e) Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích công việc của đơn vị. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.2. Trong quá trình sử dụnga) 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.1. *Tham chiếu các Điều 9, 10, 11, 17 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.*
 |

***5.1.1.2. Xây dựng và công bố***

|  |  |
| --- | --- |
| **Yêu cầu** | Quy định về xây dựng và công bố Quy chế bảo đảm an toàn thông tin |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 26. Xây dựng, rà soát, cập nhật, bổ sung Quy chế***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. Chính sách bảo đảm an toàn thông tin phải được Thanh tra tỉnh thông qua trước khi công bố áp dụng.*Tham chiếu Điều 26 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

***5.1.1.3. Rà soát, sửa đổi***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc rà soát, sửa đổi Quy chế bảo đảm an toàn thông tin |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 25. Tổ chức triển khai Quy chế***1. Quy chế này có hiệu lực thi hành kể từ ngày ký ban hành.2. Trong quá trình thực hiện nếu có vấn đề phát sinh, vướng mắc, các tổ chức, cá nhân liên quan phản ánh kịp thời về Bộ phận phụ trách để xem xét, bổ sung, sửa đổi.***Điều 26. Xây dựng, 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. Chính sách được tổ chức/ bộ phận được ủy quyền thông qua trước khi công bố áp dụng.2. Trong quá trình thực hiện Quy chế, nếu có vấn đề vướng mắc, phát sinh, các đơn vị phản ánh kịp thời về Bộ phận chuyên trách về ATTT thuộc phòng Văn hoá và Thông tin để tổng hợp báo cáo, điều chỉnh, bổ sung.*Tham chiếu các Điều 25, 26 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

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

***5.1.2.1. Đơn vị chuyên trách về an toàn thông tin***

|  |  |
| --- | --- |
| **Yêu cầu** | Thành lập hoặc chỉ định đơn vị/bộ phận chuyên trách về an toàn thông tin trong tổ chức |
| **Hiện trạng** | Đáp ứng. |
| **Phương án** | ***Điều 27. Bộ phận phụ trách về an toàn thông tin*** Giao Phòng Văn hóa và Thông tin là bộ phận chuyên trách về ATTT cho các Hệ thống thông tin của UBND huyện, chủ trì, phối hợp với các phòng nghiên cứu và đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hằng năm hoặc theo chỉ đạo của Lãnh đạo UBND huyện.*Tham chiếu Điều 27 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

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

|  |  |
| --- | --- |
| **Yêu cầu *5.1.2.2.a*** | Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 5. Phối hợp với cơ quan/tổ chức có thẩm quyền***Giao Phòng Văn hóa và Thông tin là đầu mối liên hệ, phối hợp với Sở Thông tin và Truyền thông 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 các Hệ thống thông tin; Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của các Hệ thống thông tin; Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.*Tham chiếu Điều 5 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |
| **Yêu cầu *5.1.2.2.b*** | Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 5. Phối hợp với cơ quan/tổ chức có thẩm quyền***Giao Phòng Văn hóa và Thông tin là đầu mối liên hệ, phối hợp với Sở Thông tin và Truyền thông 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 các Hệ thống thông tin; Tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin của các Hệ thống thông tin; Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.*Tham chiếu Điều 5 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

**5.1.3. Bảo đảm nguồn nhân lực**

***5.1.3.1. Tuyển dụng***

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ |
| **Hiện trạng** | Đáp ứng |
| **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.*Tham chiếu khoản 1, Điều 6 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

***5.1.3.2. Trong quá trình làm việc***

|  |  |
| --- | --- |
| **Yêu cầu****5.1.3.2.a** | Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 6. Bảo đảm nguồn nhân lực***3. 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 bộ phận, phòng, ban, đơn vị thuộc UBND huyện, UBND các xã, thị trấn 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.4. Trách nhiệm bảo đảm an toàn thông tin đối với người sử dụng:a) Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc. Trước khi tham gia vào hệ thống phải được kiểm tra khả năng đáp ứng các yêu cầu về ATTT.b) Phải thường xuyên học tập và cập nhật các quy định về ATTT, nhằm nâng cao nhận thức và trách nhiệm đảm bảo ATTT.5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:a) Cán bộ nghỉ hoặc thay đổi công việc phải được thu hồi thẻ/tài khoản truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của cơ quan.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.***Điều 17. 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) Các thiết bị đầu cuối khi kết nối phải được quản lý và cập nhật thông tin (tên, chủng loại, địa chỉ MAC, địa chỉ IP).b) 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.c) 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.d) 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.đ) Việc sử dụng các thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải thường xuyên quét virus trước khi đọc hoặc sao chép dữ liệu.e) Không sử dụng các máy tính thuộc sở hữu cá nhân (máy xách tay của cá nhân, PDA) hoặc những thiết bị lưu trữ di động cá nhân vào mục đích công việc của đơn vị. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu.2. Trong quá trình sử dụnga) 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.*Tham chiếu khoản 3, Điều 6, Điều 17 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |
| **Yêu cầu****5.1.3.2.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** | Đáp ứng |
| **Phương án** | ***Điều 6. Bảo đảm nguồn nhân lực***2. Định kỳ hằng năm bố trí kinh phí và cử cán bộ thuộc 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống tham gia các lớp đào tạo và bồi dưỡng về an toàn thông tin.*Tham chiếu khoản 2, Điều 6 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 6. Bảo đảm nguồn nhân lực***5. Quy định đối với cán bộ nghỉ hoặc thay đổi công việca) Cán bộ nghỉ hoặc thay đổi công việc phải được thu hồi dữ liệu được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chức.*Tham chiếu điểm a, khoản 5, Điều 6 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

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

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

|  |  |
| --- | --- |
| **Yêu cầu****5.1.4.1.a** | Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 7. Thiết kế, xây dựng hệ thống thông tin***1. Xây dựng các tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.*Tham chiếu khoản 1, Điều 7 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |
| **Yêu cầu****5.1.4.1.b** | Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 7. Thiết kế, xây dựng hệ thống thông tin***2. Xây dựng các tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin.*Tham chiếu khoản 2, Điều 7 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 8. Phát triển phần mềm thuê khoán***3. Phần mềm thuê khoán phải được kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.*Tham chiếu khoản 3, Điều 8 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

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

***5.1.5.1. Quản lý an toàn mạng***

|  |  |
| --- | --- |
| **Yêu cầu *5.1.5.1.a*** | Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 9. Quản lý an toàn mạng***1. Quản lý, vận hành và bảo đảm an toàn hệ thống mạnga) Hệ thống mạng phải được thiết kế thống nhất, được quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý và bảo đảm an toàn và bảo mật.b) Hệ thống mạng nội bộ (LAN) phải được bảo vệ bằng tường lửa (có thể tích hợp tường lửa trên modem hoặc router) và phân chia hệ thống mạng thành các vùng mạng quản lý theo chính sách an toàn thông tin riêng. c) Mạng không dây (WIFI), cần thiết lập các thông số an toàn và định kỳ ít nhất 3 tháng thay đổi mật khẩu truy cập nhằm tăng cường công tác bảo mật. Hệ thống mạng không dây phải được bảo vệ bởi mật khẩu an toàn.*Tham chiếu khoản 1, Điều 9 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |
| **Yêu cầu *5.1.5.1.b*** | Có quy định về cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 10. Quản lý an toàn máy chủ và ứng dụng***4. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cốTriển 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; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản như: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.*Tham chiếu khoản 4, Điều 10 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |
| **Yêu cầu *5.1.5.1.c*** | Truy cập và quản lý cấu hình hệ thống |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | **Điều 9. Quản lý an toàn mạng**2. Truy cập và quản lý cấu hình hệ thốnga) Cán bộ quản lý truy cập, khai thác thông tin 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 có trách nhiệm theo dõi và phát hiện các trường hợp truy cập hệ thống trái phép hoặc thao tác vượt quá giới hạn, 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.*Tham chiếu khoản 2, Điều 9 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 10. 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 vụa) Máy chủ phải được thiết lập chính sách xác thực và kiểm soát truy cập. Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn. Tổ chức theo dõi, giám sát tất cả các phương pháp đăng nhập từ xa, nhất là các trường hợp đăng nhập vào hệ thống với mục đích quản trị.b) Các hệ thống thông tin cần có phướng án giới hạn số lần đăng nhập, tự động khóa tài khoản khi liên tục đăng nhập sai vượt quá số lần quy định. c) 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.d) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm.- Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp.- Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng.- Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.*Tham chiếu khoản 1, Điều 10 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

***5.1.5.3. Quản lý an toàn dữ liệu***

|  |  |
| --- | --- |
| **Yêu cầu** | Có chính sách, quy trình dự phòng và khôi phục dữ liệu |
| **Hiện trạng** | Đáp ứng |
| **Phương án** | ***Điều 11. Quản lý an toàn dữ liệu***1. Yêu cầu an toàn đối với phương pháp mã hóaa) Đơn vị 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. Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ;a) Các thông tin, tài liệu, dữ liệu nhạy cảm phải được mã hóa trước khi trao đổi, truyền nhận qua mạng máy tính.b) Thực hiện các biện pháp quản lý, giám sát và kiểm soát chặt chẽ các trang/cổng thông tin điện tử cung cấp thông tin, dịch vụ, giao dịch trực tuyến cho các tổ chức, cá nhân bên ngoài.c) Thực hiện biện pháp bảo vệ trang thiết bị, phần mềm phục vụ trao đổi thông tin nội bộ nhằm hạn chế việc xâm nhập, khai thác bất hợp pháp các thông tin nhạy cảm.*Tham chiếu Điều 11 Quy chế Bảo đảm an toàn, an ninh mạng theo Quyết định số xxx/QĐ-UBND ngày dd/11/2022.* |

**PHỤ LỤC II. THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG CẤP ĐỘ 1**

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

Phương án bảo đảm an toàn thông tin cấp độ 1 được thuyết minh như dưới đây:

**5.2.1. Bảo đảm an toàn mạng**

***5.2.1.1. Thiết kế hệ thống***

a) Thiết kế các vùng mạng trong hệ thống theo chức năng, bao gồm các vùng mạng:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Vùng mạng nội bộ | Có | Cung cấp kết nối mạng cho các máy trạm và các thiết bị đầu cuối, các thiết bị khác của người sử dụng vào hệ thống |
| 2 | Vùng mạng biên | Có | Cung cấp các kết nối hệ thống ra bên ngoài Internet và các mạng khác |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn  | Có | Các thiết bị hệ thống/máy chủ được thiết lập cấu hình cho phép quản trị từ xa an toàn.Sử dụng tường lửa Firewall/ Modem có tích hợp tính năng VPN quản lý truy cập, quản trị hệ thống từ xa an toàn. Tính năng VPN này được cấu hình trực tiếp trên thiết bị Firewall/ Modem, quản lý truy cập từ bên ngoài vào vùng mạng nội bộ |
| 2 | Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập  | Có | Truy cập giữa các vùng mạng được quản lý và phòng chống xâm nhập sử dụng Firewall/ Modem có tích hợp chức năng phòng chống xâm nhập IPS. |
| 3 | Phương án phòng chống mã độc cho máy chủ và máy trạm  |  | Sử dụng sản phẩm Phòng chống mã độc hoặc phương án tương đương (Giải pháp Antivirus) |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet | Có | Hệ thống được thiết lập chỉ cho phép kết nối mạng có hỗ trợ mã hóa, xác thực khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet thông qua Firewall/ Modem |
| 2 | Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài | Có | Hệ thống được thiết lập chỉ cho phép kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể thông qua Firewall/ Modem |

***5.2.1.3. Nhật ký hệ thống***

|  |  |
| --- | --- |
| **Yêu cầu** | Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị mạng chính |
| **Thiết bị** |
| Firewall/ Modem | Ghi nhật ký theo mặc định của thiết bị |
| Firewall01/Fortigate | Ghi nhật ký theo mặc định của thiết bị |
| Switch L3/Cisco | Ghi nhật ký theo mặc định của hệ điều hành |
| Switch L2/Cisco | Ghi nhật ký theo mặc định của thiết bị |
| Wifi/TPLink | Ghi nhật ký theo mặc định của thiết bị |
| Hệ thống máy trạm (máy tính cá nhân) | Ghi nhật ký theo mặc định của hệ điều hành |

***5.2.1.4. Phòng chống xâm nhập***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có phương án phòng chống xâm nhập để bảo vệ vùng DMZ | Có | Hệ thống sử dụng tường lửa tích hợp trong thiết bị Modem/Router và Firewall ngăn chặn tất cả truy cập từ mạng Internet vào vùng mạng nội bộ và vùng mạng wifi công cộng. |
| 2 | Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng | Có | Hệ thống sử dụng tường lửa tích hợp trong thiết bị Modem/Router và Firewall ngăn chặn tất cả truy cập từ mạng Internet vào vùng mạng nội bộ và vùng mạng wifi công cộng. |

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

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Cấu hình chức năng xác thực trên các thiết bị hệ thống ( nếu hỗ trợ ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa; | Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn ( Nếu hỗ trợ ) khi truy cập, quản trị thiết bị từ xa. |
| **Thiết bị** |
| Modem/ Firewall | Xác thực bằng usename / password | Chỉ cho phép máy tính quản trị trong mạng nội bộ |
| Firewall01/Fortigate | Xác thực bằng usename / password | Chỉ cho phép máy tính quản trị trong mạng nội bộ |
| Switch L3/Cisco | Xác thực bằng usename / password | Chỉ cho phép máy tính quản trị trong mạng nội bộ |
| Switch L2/Cisco | Xác thực bằng usename / password | Chỉ cho phép máy tính quản trị trong mạng nội bộ |
| Wifi/TPLink | Xác thực bằng usename / password | Chỉ cho phép máy tính quản trị trong mạng nội bộ |
| Hệ thống máy trạm (máy tính cá nhân) | Xác thực bằng usename / password của hệ điều hành | Không cho phép truy cập từ xa |

**5.2.2. Bảo đảm an toàn máy chủ**

***5.2.2.1. Xác thực***

|  |  |  |  |
| --- | --- | --- | --- |
| **Yêu cầu** | Thiết lập chính sách xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ; | Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa | Thiết lập cấu hình máy chủ để đảm bảo an toàn mật khẩu người sử dụng |
| **Máy chủ** |
| Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7 | + | + | + |

***5.2.2.2. Kiểm soát truy cập***

|  |  |
| --- | --- |
| **Yêu cầu** | Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa |
| **Máy chủ** |
| Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7 | + |

***5.2.2.3. Nhật ký hệ thống***

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ | Đồng bộ thời gian giữa máy chủ với máy chủ thời gian |
| **Máy chủ** |
| Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7 | + | + |

***5.2.2.4. Phòng chống xâm nhập***

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ | Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ |
| **Máy chủ** |
| Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7 | + | + |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm |
| **Máy chủ** |
| Server01/Cài đặt Web-App /Vùng DMZ/HĐH Centos7 | + |

**5.2.3. Bảo đảm an toàn ứng dụng**

***5.2.3.1. Xác thực***

|  |  |  |  |
| --- | --- | --- | --- |
| **Yêu cầu** | Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng | Lưu trữ có mã hóa thông tin xác thực hệ thống | Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng |
| **Ứng dụng** |
| Cổng thông tin nội bộ | Xác thực bằng usename / password | + | + |
| Hệ thống máy trạm (máy tính cá nhân) | Xác thực bằng usename / password của hệ điều hành |  |  |
| Kết nối mạng wifi | Xác thực bằng usename / password |  |  |

***5.2.3.2. Kiểm soát truy cập***

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa | Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng |
| **Ứng dụng** |
| Cổng thông tin nội bộ | + | + |
| Hệ thống máy trạm (máy tính cá nhân) | Không cho phép | Thiết lập thời gian chờ để khoá màn hình |

***5.2.3.3. Nhật ký hệ thống***

|  |  |
| --- | --- |
| **Yêu cầu** | Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng. |
| **Ứng dụng** |
| Cổng thông tin nội bộ | + |
| Hệ thống máy trạm (máy tính cá nhân) | Ghi nhật ký theo mặc định của hệ điều hành |

**5.2.4. Bảo đảm an toàn dữ liệu**

***5.2.4.1. Sao lưu dự phòng***

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Thực hiện sao lưu dự phòng các thông tin, dữ liệu quan trọng trên hệ thống. | có | Dữ liệu được nén và được lưu trữ mã hóa sử dụng EAS 256 |

**PHỤ LỤC I**

**Danh mục các thiết bị sử dụng trong hệ thống**

1. Danh mục thiết bị sử dụng trong hệ thống của UBND xã ABC

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên thiết bị/****Chủng loại** | **Vị trí triển khai** | **Mục đích sử dụng** |
| 1 | Modem/Router/Firewall | Vùng mạng biên | Định tuyến hệ thống mạng nội bộ của cơ quan ra các mạng bên ngoài và mạng Internet, SLCD; Quản lý truy cập và bảo vệ vùng mạng nội bộ |
| 2 | Thiết bị chuyển mạch Switch | Vùng mạngnội bộ | Dùng để kết nối các đoạn mạng đến các toà nhà, các tầng trong hệ thống mạng nội bộ |
| 3 | Bộ chuyển đổi quang điện 10/100/1000 Mbps | Vùng mạngnội bộ | Chuyển đổi tín hiệu từ dạng quang sang dạng điện (và ngược lại) |
| 4 | Thiết bị Wifi | Vùng mạngnội bộ | Cung cấp kết nối mạng cho các thiết bị di động của cơ quan (laptop, điện thoại...) |
| 5 | Camera an ninh | Vùng mạngnội bộ | Dùng để giám sát an ninh cơ quan |
| 6 | Thiết bị chuyển mạch Switch | Vùng mạng Publish / Guest | Dùng để kết nối các đoạn mạng đến các toà nhà, các tầng trong hệ thống mạng nội bộ |
| 7 | Thiết bị Wifi | Vùng mạng Publish / Guest | Cung cấp kết nối internet cho khách, người dân đến làm việc tại đơn vị |

1. Danh mục thiết bị sử dụng trong hệ thống của UBND xã XYZ

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên thiết bị/****Chủng loại** | **Vị trí triển khai** | **Mục đích sử dụng** |
| 1 | Modem/Router/Firewall | Vùng mạng biên | Định tuyến hệ thống mạng nội bộ của cơ quan ra các mạng bên ngoài và mạng Internet, SLCD; Quản lý truy cập và bảo vệ vùng mạng nội bộ |
| 2 | Thiết bị chuyển mạch Switch | Vùng mạngnội bộ | Dùng để kết nối các đoạn mạng đến các toà nhà, các tầng trong hệ thống mạng nội bộ |
| 3 | Bộ chuyển đổi quang điện 10/100/1000 Mbps | Vùng mạngnội bộ | Chuyển đổi tín hiệu từ dạng quang sang dạng điện (và ngược lại) |
| 4 | Thiết bị Wifi | Vùng mạngnội bộ | Cung cấp kết nối mạng cho các thiết bị di động của cơ quan (laptop, điện thoại...) |
| 5 | Camera an ninh | Vùng mạngnội bộ | Dùng để giám sát an ninh cơ quan |
| 6 | Thiết bị chuyển mạch Switch | Vùng mạng Publish / Guest | Dùng để kết nối các đoạn mạng đến các toà nhà, các tầng trong hệ thống mạng nội bộ |
| 7 | Thiết bị Wifi | Vùng mạng Publish / Guest | Cung cấp kết nối internet cho khách, người dân đến làm việc tại đơn vị |

1. Danh mục thiết bị sử dụng trong hệ thống của UBND xã …

**PHỤ LỤC II**

**MÔ HÌNH KẾT NỐI VẬT LÝ CỤ THỂ**

1. Mô hình kết nối vật lý UBND xã ABC



1. Mô hình kết nối vật lý UBND xã XYZ



1. Mô hình kết nối vật lý UBND xã ….