**ỦY BAN NHÂN DÂN**

**HUYỆN KON RẪY**

HỒ SƠ

ĐỀ XUẤT CẤP ĐỘ

HỆ THỐNG THÔNG TIN HUYỆN

KON RẪY

Kon Rẫy – 2023

**THUẬT NGỮ, TỪ VIẾT TẮT**

|  |  |  |
| --- | --- | --- |
| **STT** | **Từ viết tắt** | **Nghĩa đầy đủ** |
| 1 | CNTT | Công nghệ thông tin |
| 2 | CSDL | Cơ sở dữ liệu |
| 3 | HSĐXCĐ | Hồ sơ đề xuất cấp độ |
| 4 | LAN | Mạng nội bộ |
| 5 | WAN | Mạng tin học diện rộng |

## PHẦN I

## THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

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

**\* Tên Tổ chức: Ủy ban nhân dân huyện Kon Rẫy .**

-Quy định chức năng, nhiệm vụ và quyền hạn: Ủy ban nhân dân huyện Kon Rẫy là đơn vị hành chính cấp huyện, thực hiện chức năng, nhiệm vụ, quyền hạn được quy định tại Điều 28 và Điều 29 của Luật Tổ chức chính quyền địa phương năm 2015.

- Người đại diện: Võ Văn Lương – Chủ tịch UBND huyện.

- Địa chỉ: thôn 1, xã Tân Lập, huyện Kon Rẫy, tỉnh Kon Tum.

- Thông tin liên hệ: Số điện thoại: 0914080157.

- Thư điện tử: ubnd.kry@kontum.gov.vn.

2. **Thông tin Đơn vị vận hành**

- Tên Đơn vị vận hành: Phòng Văn hóa và Thông tin, Văn phòng HĐND - UBND huyện.

- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 01/2023/QĐ-UBND ngày 10/3/2023 của UBND huyện về Quyết định ban hành quy định về chức năng, nhiệm vụ, quyền hạn và tổ chức của Phòng Văn hóa và Thông tin. Quyết định số 02/2023/QĐ-UBND ngày 10/3/2023 của UBND huyện về Quyết định ban hành quy định về chức năng, nhiệm vụ, quyền hạn và tổ chức của Văn phòng HĐND - UBND huyện.

- Người đại diện: Ông Phạm Viết Thạch, Chức vụ: Trưởng phòng Văn hóa và Thông tin, Ông Trần Khắc Hà, Chức vụ: Chánh Văn phòng HĐND – UBND huyện.

- Địa chỉ: thôn 1, xã Tân Lập, huyện Kon Rẫy, tỉnh Kon Tum.

- Thông tin liên hệ:

+ Phòng Văn hóa và Thông tin: Số điện thoại: 0935785899, Thư điện tử: thachpv.kry@kontum.gov.vn

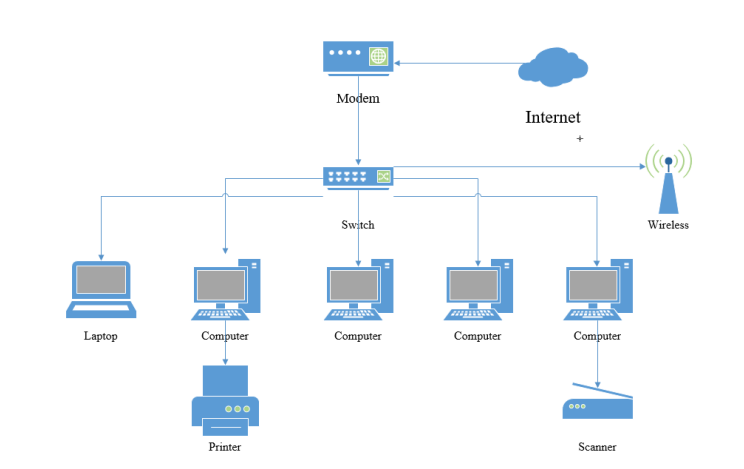
+ Văn phòng HĐND-UBND huyện: Số điện thoại 0339666468, Thư điện thử: vphdndubnd.kry@kontum.gov.vn.

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

**-** Phạm vi, quy mô của Hệ thống thông tin: Hệ thống thông tin UBND huyện Kon Rẫy được thiết lập để phục vụ công tác ứng dụng công nghệ thông tin, chuyển đổi số của UBND huyện Kon Rẫy.

**-** Đối tượng phục vụ của hệ thống: Công chức, viên chức, người lao động và cơ quan, tổ chức khác liên quan đến việc cung cấp ứng dụng CNTT, chuyển đổi số của UBND huyện Kon Rẫy.

1. **Mô tả cấu trúc của hệ thống** 
   1. **Mô hình logic tổng thể**



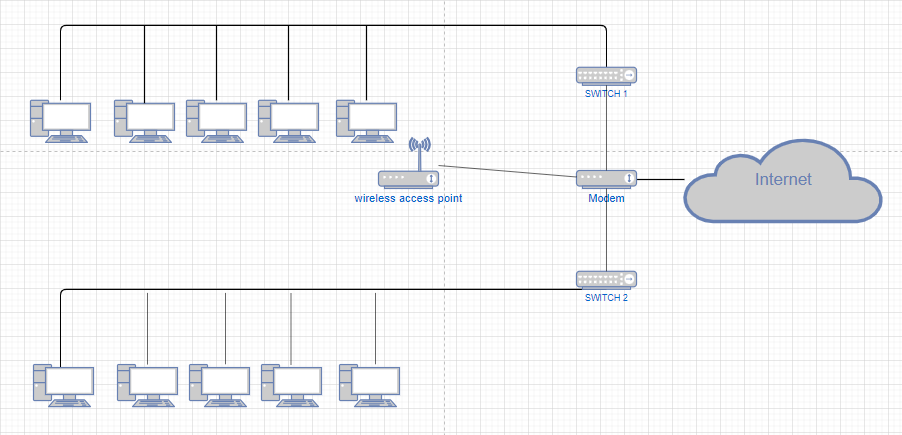
Các vùng mạng được thiết kế như sau:

Vùng mạng biên được đặt các thiết bị Router, Firewall để kết nối hệ thống ra các mạng bên ngoài và mạng Internet.

Vùng DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet.

Vùng máy chủ nội bộ (Server Farm) đặt các máy chủ nội bộ, máy chủ cơ sở dữ liệu, cung cấp các dịch vụ/chuyên ngành cho người sử dụng trong hệ thống.

* 1. **Mô hình kết nối vật lý**



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

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Tên thiết bị/Chủng loại** | **Vị trí triển khai** | **Mục đích sử dụng** |
| 1 | Modem Draytek Vigor2912 | Vùng mạng biên | Kết nối và định tuyến động với các Router của 1 ISP |
| 2 | Switch 1: Dlink 10/100Mbps | Vùng mạng nội bộ | Kết nối với Modem và chia sẻ kết nối internet cho các máy trạm |
| 3 | Switch 2: Dlink 10/100Mbps | Vùng mạng nội bộ | Kết nối với Modem và chia sẻ kết nối internet cho các máy trạm |
| 4 | Access point Tplink Deco M4 | Vùng mạng không dây | Kết nối với Modem và chia sẻ kết nối internet không dây |

* 1. **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 | Quản lý văn bản và điều hành | Web Server (Máy Ảo)/Cài đặt Web-App/Vùng DMZ/Window Server 2019  Database Server (Máy Ảo)/ Cài đặt SQL server 2019/Vùng máy chủ nội bộ/Window Server 2019 | Quản lý hệ thống văn bản và điều hành |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Vùng mạng** | **IP Private** | **IP Public** |
| 1 | Vùng máy DMZ | 172.16.1.0/24 |  |
| 2 | Vùng máy chủ nội bộ | 172.18.0.1/24 |  |
| 3 | Vùng mạng biên | 103.16.0.0/24 | 103.16.0.0/24 |
| 4 | Vùng mạng LAN | 192.168.0.1/24 |  |

## 

## 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 quản lý văn bản và điều hành | 2 | Điểm a Khoản 2 Điều 8 Nghị định 85/2016/NĐ-CP |

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

Hệ thống thông tin UBND huyện được xây dựng để phục vụ hoạt động nội bộ của cơ quan, tổ chức và có xử lý thông tin riêng, thông tin cá nhân của người sử dụng nhưng không xử lý thông tin bí mật nhà nước theo quy định của pháp luật, căn cứ theo quy định tại Khoản 1 Điều 8 Nghị định 85/2016/NĐ-CP, hệ thống này được đề xuất cấp độ 2.

## PHẦN III

## THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN

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

**1. Phạm vi chính sách an toàn thông tin**

Kế hoạch ứng dụng công nghệ thông tin; Kế hoạch phát triển chính quyền số và bảo đảm an toàn thông tin mạng hàng năm; Kế hoạch Chuyển đổi số hàng năm của UBND huyện; Quy chế đảm bảo an toàn, an ninh thông tin của UBND huyện.

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

- Bộ phận chuyên trách về an toàn thông tin: Phòng Văn hóa và Thông tin huyện và Văn phòng HĐND-UBND huyện là đơn vị chịu trách nhiệm chuyên trách về an toàn thông tin của UBND huyện.

- Thường xuyên kiểm tra mức độ an toàn thông tin.

- Cập nhật các phần mềm diệt virus.

- Kiểm tra và cập nhật các bản vá lỗi để sửa chữa các lỗ hỏng bảo mật.

**3. Bảo đảm nguồn nhân lực**

- Xây dựng yêu cầu về vị trí việc làm về an toàn thông tin.

- Cán bộ được giao nhiệm vụ 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 việc làm.

- Nguồn nhân lực đảm bảo an toàn thông tin phải được thường xuyên tập huấn và đào tạo kiến thức an toàn thông tin.

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

- Hệ thống thông tin phải có tài liệu mô tả thiết kế, quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

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

**5. Quản lý vận hành hệ thống:** Quản lý an toàn ứng dụng.

**6. Quản lý an toàn dữ liệu**

- Thực hiện quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.

- 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.

**7. Quản lý an toàn mạng**

- Hệ thống mạng phải được thiết kế thống nhất, cùng kết hợp và hỗ trợ, tương tác hoạt động với nhau, được tổ chức quản lý định danh, xác thực đối với tất cả người sử dụng nhằm mục đích quản lý hệ thống chặt chẽ, bảo đảm an toàn và bảo mật.

- Hệ thống mạng phải được thiết lập cấu hình để: Kiểm soát truy cập từ bên trong mạng; Kết nối về hệ thống giám sát tập trung; Phòng chống xâm nhập giữa các vùng mạng; Phòng chống phần mềm độc hại trên môi trường mạng.

- Các thiết bị mạng phải được cấu hình chức năng xác thực; Chỉ cho phép sử dụng các kết nối mạng an toàn (nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa; Giới hạn 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; Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng.

- Hệ thống mạng phải được trang bị hệ thống kỹ thuật, công nghệ hiện đại để thường xuyên, liên tục quản lý, giám sát, kiểm soát mạng nhằm phát hiện, ngăn chặn các truy cập trái phép của người sử dụng, tin tặc tấn công; triển khai cơ chế phòng chống vi rút tin học tại các máy trạm khác trong hệ thống.

- Việc thanh lý, tiêu hủy thiết bị, vật mang thông tin trong mạng phải đảm bảo yêu cầu không để lộ, lọt thông tin Nhà nước. Phải có quy trình cụ thể và phải lưu giữ hồ sơ, biên bản việc thanh lý, tiêu hủy.

- Đối với các thiết bị mạng chính:

+ Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT, phảỉ xây dựng ít nhất 02 thiết bị chống sét: một cho một đường cung cấp điện và một đường của mạng nội bộ (LAN).

+ Thiết bị chuyển mạch (switch): Thiết bị chuyển mạch mạng tin học của các cơ quan phải đảm bảo khả năng cung cấp các chức năng quản trị nhằm tăng cường độ an toàn và bảo mật cho hệ thống mạng như: cung cấp khả năng từ chối các kết nối không mong muốn vào hệ thống trên từng cổng, quy định địa chỉ IP cho từng cổng và khống chế số lượng kết nối vào hệ thống mạng nội bộ thông qua thiết bị chuyển mạch. Phải có ít nhất 01 thiết bị chuyển mạch có hỗ trợ định tuyến IP (IP routing) cho mỗi mạng nội bộ, hỗ trợ chức năng điều khiển truy cập (Access Control List), hỗ trợ chức năng xác thực thiết bị và nguời sử dụng (User & Device Authentication) và chức năng bảo mật quản trị mạng

- Có biện pháp bảo vệ, dự phòng, phòng chống các nguy cơ do mất cắp, cháy nổ, ngập lụt… các thảm họa khác do thiên nhiên hoặc con nguời gây ra và các phuơng án khôi phục hệ thống sau thảm họa.

**7.1 Quản lý sự cố an toàn thông tin**

- Đơn vị/bộ phận chuyên trách về an toàn thông tin có trách nhiệm:

+ Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tuớng Chính phủ ngày 16/3/2017 quy định về hệ thống phuơng 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.

+ 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.

- Trách nhiệm của nguời dùng: Thông tin, báo cáo kịp thời cho cán bộ chuyên trách về ATTT của cơ quan khi phát hiện các sự cố gây mất ATTT trong quá trình tham gia vào hệ thống thông tin của đơn vị; Phối hợp tích cực trong suốt quá trình giải quyết và khắc phục sự cố.

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

- Kết nối máy tính/thiết bị đầu cuối của người sử dụng vào hệ thống:

+ 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.

+ 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.

- Trong quá trình sử dụng:

+ 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;

+ Có trách nhiệm tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng;

+ 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;

+ Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng được tỉnh hoặc đơn vị chuyên môn tổ chức.

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

***1. Bảo đảm an toàn mạng***

a) Thiết kế hệ thống

- Vùng mạng nội bộ: Vùng mạng cung cấp cho các máy trạm trong cơ quan UBND huyện.

- Vùng mạng biên: Kết nối hệ thống với mạng Internet và mạng diện rộng

- Vùng mạng không dây: Cấu hình riêng dãy địa chỉ IP để không ảnh hưởng đến hệ thống.

b) Kiểm soát truy cập từ bên ngoài mạng: Chưa có chính sách.

c) Kiểm soát truy cập từ bên trong mạng: Chưa có chính sách.

d) Nhật ký hệ thống: Hệ thống nhật ký hiện mới chỉ bật tính năng trên thiết bị Router; các thiết bị mạng khác chưa có chức năng này.

e) Phòng chống xâm nhập: Chưa có chính sách.

f) Phòng chống phần mềm độc hại trên môi trường mạng: Đã triển khai phần mềm phòng chống mã độc tập trung đảm bảo theo Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại.

g) Bảo vệ thiết bị hệ thống: Đã thiết lập chức năng cho phép, hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa trên thiết bị Router.

***2. Bảo đảm an toàn dữ liệu***

Thực hiện sao lưu các dữ liệu quan trọng của cơ quan tại các vị trí như văn thư, kế toán… sang các thiết bị lưu trữ độc lập.

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống thông tin UBND huyện Kon Rẫy sẽ bao gồm các thuyết minh thành phần sau:

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

## 

## PHỤ LỤC I

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

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

**1.1. Chính sách an toàn thông tin**

|  |  |
| --- | --- |
| **Yêu cầu** | Xây dựng chính sách an toàn thông tin |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | **Quản lý an toàn mạng**   1. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống. 2. Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần. 3. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc. 4. Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống. 5. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:    1. Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như USB, DVD hoặc SAN.    2. Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. 6. Truy cập và quản lý cấu hình hệ thống:    1. Cấu hình hệ thống tư xa phải sử dụng các giảo thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN.    2. Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN.    3. Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập. |
|  | **Quản lý an toàn máy chủ và ứng dụng**  Quy định về quản lý an toàn máy chủ và ứng dụng:  1. Quy định với máy chủ   1. Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng. 2. Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ 01 tháng/lần. 3. Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. 4. Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và xóa sạch dữ liệu.   đ) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.   1. Quy định với ứng dụng:    1. Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.    2. Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Có phương án bảo mật thông tin liên lạc và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.    3. Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin 2 năm/lần hoặc khi thay đổi, nâng cấp mở rộng. 2. Truy cập mạng của máy chủ:    1. Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống.    2. Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có).    3. Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN.   4. Truy cập và quản trị máy chủ và ứng dụng:  a) Định kỳ 03 tháng thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.   1. Chỉ cấp quyền quản lý máy chủ và ứng dụng cho cán bộ quản trị theo chức năng nhiệm vụ được giao. 2. Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN. 3. Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN. 4. Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:    1. Định kỳ hàng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập.    2. Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn.    3. Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.   **Quản lý an toàn dữ liệu**   * + 1. Quy định dự phòng và khôi phục dữ liệu:        1. Định kỳ hàng tuần phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập.        2. Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn.        3. Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập.   2. Định kỳ hàng tháng 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.  3. Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập.  **Quản lý sự cố an toàn thông tin**  1. Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác.   1. Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố. 2. Liên hệ với đầu mối ứng cứu sự cố theo thông tin đưa ra dưới đây:   a) Phòng Văn hóa và Thông tin  - Người liên hệ: Hoàng Thị Hương  + Số điện thoại: 0346391161  + Email: huonght.kry@kontum.gov.vn   1. Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)    * Người liên hệ/bộ phận: Phòng Ứng cứu sự cố    * Số điện thoại: 0869 100 317    * Email: [ir@vncert.vn](mailto:ir@vncert.vn)    * Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: https://irlab.vn    * Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn   **Quản lý an toàn người sử dụng đầu cuối**   1. Khi kết nối thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu. 2. 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 mạng quản trị hoặc nghiệp vụ. Hạn chế tối đa việc sử dụng các thiết bị lưu trữ ngoài để sao chép, di chuyển dữ liệu. 3. 3. Thiết lập mạng công cộng cho 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 và có quản lý truy cập vùng mạng này với các vùng mạng khác trong hệ thống. 4. 4. Máy tính người sử dụng phải được thiết lập chế độ cập nhật bản vá tự động và phần mềm phòng chống mã độc. |

**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** | **Đã đáp ứng** |
| **Phương án** | Tiếp tục triển khai thực Quy chế bảo đảm an toàn thông tin trình người đứng đầu đơn vị vận hành ban hành. |

**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** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Định kỳ 03 năm hoặc khi có thay đổi Quy chế bảo đảm an toàn thông tin kiểm tra lại tính phù hợp và thực hiện rà soát, cập nhật, bổ sung. |

**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 |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Đã xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Giao Phòng Văn hóa và Thông tin là bộ phận chuyên trách về an toàn thông tin, có trách nhiệm bảo đảm an toàn thông tin cho hệ thống thông tin. |

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

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Giao Phòng Văn hóa và 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. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có đầu mối liên hệ, phối hợp với các cơ quan, tổ chức trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  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:  a) Phòng Văn hóa và Thông tin  - Người liên hệ: Hoàng Thị Hương  + Số điện thoại: 0346391161  + Email:huonght.kry@kontum.gov.vn   1. Cục An toàn thông tin/Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC)    * Người liên hệ/bộ phận: Phòng Ứng cứu sự cố    * Số điện thoại: 0869 100 317    * Email: [ir@vncert.vn](mailto:ir@vncert.vn)    * Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: <https://irlab.vn>. Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Bộ phận chuyên trách về an toàn thông tin là đầu mối tham gia các hoạt động, công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền |

**3. Bảo đảm nguồn nhân lực**

**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** | Tiếp tục thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Quy định về tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ: Cán bộ được tuyển dụng vào vị trí làm về an toàn thông tin có trình độ, chuyên ngành phù hợp với vị trí tuyển dụng. |

**3.2. Trong quá trình làm việc**

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc thực hiện nội quy, quy chế bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục triển khai thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc:  Trách nhiệm bảo đảm an toàn thông tin cho người sử dụng, cán bộ quản lý và vận hành hệ thống   1. Với người sử dụng:   - Người sử dụng có trách nhiệm đảm bảo ATTT đối với từng vị trí công việc.  - Phải được thường xuyên tổ chức quán triệt các quy định về ATTT, nhằm nâng cao nhận thức về trách nhiệm đảm bảo ATTT.  - Phải có trách nhiệm tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.  b) Với cán bộ quản lý và vận hành hệ thống: Cán bộ quản lý và vận hành hệ thống 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.  - Cán bộ quản lý và vận hành hệ thống phải tổ chức quản lý định danh đối với tất cả người dùng tham gia sử dụng hệ thống thông tin. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có kế hoạch và định kỳ hàng năm tổ chức phổ biến, tuyên truyền nâng cao nhận thức về an toàn thông tin cho người sử dụng |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Kế hoạch và định kỳ hàng năm tổ chức đào tạo về an toàn thông tin cho 03 nhóm đối tượng bao gồm: cán bộ kỹ thuật, cán bộ quản lý và người sử dụng trong hệ thống. |

**3.2.c. Chấm dứt hoặc thay đổi công việc**

|  |  |
| --- | --- |
| **Yêu cầu** | 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** |
| **Phương án** | Tiếp tục triển khai thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quy định đối với cán bộ nghỉ hoặc thay đổi công việc:   1. Cán bộ nghỉ hoặc thay đổi công việc phải thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác thuộc sở hữu của tổ chức. 2. Bộ phận chuyên trách vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc. |
| **Yêu cầu** | Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc. |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách về an toàn thông tin 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. |

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

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

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách xây dựng tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin và thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách xây dựng tài liệu mô tả thiết kế và các thành phần của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách xây dựng tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Bộ phận chuyên trách xây dựng tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin của hệ thống thông tin thuyết minh trong Hồ sơ đề xuất cấp độ của hệ thống. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống |
| **Hiện trạng** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau: Bộ phận chuyên trách 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, báo cáo Lãnh đạo quyết định trước khi thực hiện thay đổi. |

**5. Phát triển phần mềm thuê khoán**

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quy định đối với việc phát triển phần mềm thuê khoán:  Yêu cầu có biên bản, hợp đồng và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán. |

**5.2. Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm**

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm |
| **Hiện trạng** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quy định đối với việc phát triển phần mềm thuê khoán:   1. Các nhà phát triển cung cấp mã nguồn phần mềm cho bộ phận chuyên trách. 2. Bộ phận chuyên trách có trách nhiệm quản lý và lưu trữ mã nguồn an toàn. |

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

**6.1. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng**

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về việc thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quy định đối với việc thử nghiệm và nghiệm thu hệ thống:  1. Bên triển khai xây dựng kế hoạch, nội dung thử nghiệm hệ thống trước khi thực hiện thử nghiệm và nghiệm thu hệ thống.  2. Đơn vị vận hành thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác theo phương án thiết kế được phê duyệt trong Hồ sơ đề xuất cấp độ. |

**6.2** **Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống**

|  |  |
| --- | --- |
| **Yêu cầu** | Có yêu cầu về nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: Bộ phận chuyên trách và bên triển khai hệ thống xây dựng kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống, trình Lãnh đạo đơn vị phê duyệt trước khi đưa hệ thống vào vận hành, khai thác. |

**6.3. Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống**

|  |  |
| --- | --- |
| **Yêu cầu** | Có bộ phận có trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Quy định đối với việc thử nghiệm và nghiệm thu hệ thống: Bộ phận chuyên trách phối hợp với bên triển khai hệ thống thực hiện thử nghiệm và nghiệm thu hệ thống, trước khi đưa vào vận hành, khai thác. |

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

**7.1. Quản lý an toàn mạng**

**7.1.a Quản lý, vận hành hoạt động bình thường của hệ thống**

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quy định về quản lý an toàn mạng:   1. Hoạt động của hệ thống phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của hệ thống. 2. Toàn bộ cấu hình hệ thống phải được sao lưu, dự phòng trên thiết bị hoặc hệ thống lưu trữ độc lập, định kỳ 01 tháng/lần. 3. Khi thực hiện nâng cấp, thay đổi cấu hình hệ thống phải thực hiện ngoài giờ làm việc.   Phải kiểm tra hoạt động tổng thể của hệ thống sau khi thay đổi cấu hình hoặc nâng cấp hệ thống. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về cập nhật; sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: Định kỳ hàng tháng hoặc khi có thay đổi, bộ phận chuyên trách thực hiện sao lưu, dự phòng hệ thống trên hệ thống độc lập như USB, DVD hoặc SAN.  Các dữ liệu sau yêu cầu sao lưu, dự phòng: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ. |

**7.2.c. Truy cập và quản lý cấu hình hệ thống**

|  |  |
| --- | --- |
| Yêu cầu | Truy cập và quản lý cấu hình hệ thống |
| **Hiện trạng** | **Chưa đáp ứng** |
| **Phương án** | Truy cập và quản lý cấu hình hệ thống: Cấu hình hệ thống tư xa phải sử dụng các giảo thức bảo mật có mã hóa thông tin như SSL, TSL, SSH, VPN. Khi cấu hình hệ thống từ bên ngoài phải thông qua kết nối VPN. Toàn bộ cấu hình hệ thống phải được lưu trên thiết bị hoặc hệ thống lưu trữ độc lập. |

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

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quy định về quản lý an toàn máy chủ và ứng dụng:  1. Quy định với máy chủ   1. Hoạt động của máy chủ phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng. 2. Ảnh hệ điều hành phải được sao lưu dự phòng trên hệ thống lưu trữ độc lập định kỳ 01 tháng/lần. 3. Máy chủ phải được nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng. 4. Việc kết nối, gỡ bỏ máy chủ khỏi hệ thống phải được sự cho phép của Thủ trưởng đơn vị và xóa sạch dữ liệu.   đ) Có tài liệu liệt kê, cài đặt với những phần mềm hệ thống cài trong máy chủ.   1. Quy định với ứng dụng:    1. Hoạt động của ứng dụng phải được giám sát thường xuyên, liên tục, bảo đảm tính khả dụng của ứng dụng.    2. Ứng dụng phải được thiết lập chính sách xác thực; Kiểm soát truy cập; Có phương án bảo mật thông tin liên lạc và biện pháp bảo đảm an toàn ứng dụng và mã nguồn.    3. Ứng dụng phải được định kỳ kiểm tra đánh giá an toàn thông tin 2 năm/lần hoặc khi thay đổi, nâng cấp mở rộng. |

**8.1.a.** **Truy cập mạng của máy chủ**

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định quản lý truy cập mạng của máy chủ |
| **Hiện trạng** | **Chưa đáp ứng** |
| **Phương án** | 1. Truy cập mạng của máy chủ:    1. Kết nối, truy cập máy chủ phải được kiểm soát bởi tường lửa hệ thống.    2. Chỉ mở cổng quản trị hệ thống từ vùng mạng LAN hoặc vùng mạng quản trị (nếu có).   Truy cập quản trị máy chủ từ bên ngoài mạng phải qua kênh kết nối VPN. |

**8.1.b. Truy cập và quản trị máy chủ và ứng dụng**

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định quản lý truy cập và quản trị máy chủ và ứng dụng |
| **Hiện trạng** | **Chưa đáp ứng** |
| **Phương án** | 1. Truy cập và quản trị máy chủ và ứng dụng:    1. Định kỳ 03 tháng thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng.    2. Chỉ cấp quyền quản lý máy chủ và ứng dụng cho cán bộ quản trị theo chức năng nhiệm vụ được giao.    3. Truy cập quản trị máy chủ và ứng dụng phải qua giao thức mã hóa như SSL, TLS, SSH và VPN.    4. Truy cập quản trị máy chủ và ứng dụng từ bên ngoài mạng phải qua kênh kết nối VPN. |

**8.1.c. Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố**

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố |
| **Hiện trạng** | Chưa đáp ứng |
| **Phương án** | Quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố:   1. Định kỳ hàng tháng hoặc khi nâng cấp ứng dụng phải sao lưu, dự phòng mã nguồn ứng dụng và cơ sở dữ liệu trên thiết bị hoặc hệ thống độc lập. 2. Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn. 3. Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản truy lý cập |

**9. Quản lý an toàn dữ liệu**

**9.1. Chính sách, quy trình dự phòng và khôi phục dữ liệu**

|  |  |
| --- | --- |
| **Yêu cầu** | Có chính sách, quy trình dự phòng và khôi phục dữ liệu |
| **Hiện trạng** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:   1. Quy định dự phòng và khôi phục dữ liệu:    1. Định kỳ hàng tuần phải sao lưu, dự phòng cơ sở dữ liệu và dữ liệu nghiệp vụ (nếu có) trên thiết bị hoặc hệ thống độc lập.    2. Dữ liệu lưu trữ phải được mã hóa cùng mã kiểm tra tính nguyên vẹn.    3. Dữ liệu lưu trữ phải được quản lý theo phiên bản và có quản lý truy cập. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định định kỳ hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ |
| **Hiện trạng** | **Chưa đáp ứng** |
| **Phương án** | Xây dựng Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Định kỳ hàng tháng hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.  Bản sao lưu được lưu trữ trên thiết bị hoặc hệ thống độc lập. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Phương án quản lý sự cố an toàn thông tin mạng |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  - Thực hiện cô lập hệ thống, ngắt kết nối với các hệ thống liên quan khác.  - Khi có sự cố an toàn thông tin xảy ra, bộ phận chuyên trách phải sao lưu, dự phòng toàn bộ hiện trạng hệ thống trước khi xử lý sự cố.  - Báo cáo sự cố qua nền tảng điều phối, xử lý sự cố an toàn thông tin mạng quốc gia: <https://irlab.vn>  - Báo cáo sự cố qua website của VNCERT/CC: https://vncert.vn |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định về quản lý truy cập, sử dụng tài nguyên nội bộ |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục triển khai thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quản lý an toàn người sử dụng đầu cuối:   1. Khi kết nối thiết bị lưu trữ ngoài như ổ cứng di động, các loại thẻ nhớ, thiết bị lưu trữ USB,... phải quét virus trước khi đọc hoặc sao chép dữ liệu. 2. 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 mạng quản trị hoặc nghiệp vụ. 3. Thiết lập mạng công cộng cho 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 và có quản lý truy cập vùng mạng này với các vùng mạng khác trong hệ thống.   4. Máy tính người sử dụng phải được thiết lập chế độ cập nhật bản vá tự động và phần mềm phòng chống mã độc. |

**12. Phương án Quản lý rủi ro an toàn thông tin**

|  |  |
| --- | --- |
| **Yêu cầu** | Có chính sách, quy trình quản lý quản lý rủi ro an toàn thông tin |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Tiếp tục triển khai thực hiện Quy chế bảo đảm an toàn thông tin cho hệ thống, bao gồm những nội dung sau:  Quy định về Quản lý rủi ro an toàn thông tin:  Đơn vị vận hành xây dựng và ban hành Hồ sơ Quản lý rủi ro an toàn thông tin bao gồm các nội dung sau:  1. Danh mục tài sản thông tin, dữ liệu có trong hệ thống  2. Đánh giá các rủi ro an toàn thông tin đối với mỗi loại tài sản.  3. Có phương án dự phòng và khôi phục sau sự cố đối với thông tin, dữ liệu và ứng dụng. |

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

|  |  |
| --- | --- |
| **Yêu cầu** | Có quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ |
| **Hiện trạng** | **Đáp ứng** |
| **Phương án** | Quy định, quy trình về Kết thúc vận hành, khai thác, thanh lý, hủy bỏ bao gồm các nội dung sau:   1. Thiết bị CNTT có chứa dữ liệu (máy tính, thiết bị lưu trữ, ...) khi bị hỏng phải được cán bộ vận hành kiểm tra, sửa chữa, khắc phục. Phải có biện pháp kiểm tra, giám sát đảm bảo không để lọt lộ thông tin hay lây nhiễm mã độc đối với máy tính mang ra bên ngoài sửa chữa, bảo hành. 2. Trước khi tiến hành thanh lý/loại bỏ thiết bị công nghệ thông tin cũ, phải áp dụng các biện pháp kỹ thuật xoá bỏ hoàn toàn dữ liệu người dùng đã tạo ra, đảm bảo không thể phục hồi.   3. Các phương tiện và thiết bị CNTT: Máy tính cá nhân (PC), máy tính xách tay, máy chủ, các thiết bị mạng, phương tiện lưu trữ như CD/DVD, thẻ nhớ, ổ cứng phải xóa sạch dữ liệu khi chuyển giao hoặc thay đổi mục đích sử dụng. |

# 

# PHỤ LỤC II

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

**1. Bảo đảm an toàn mạng**

**1.1. Thiết kế hệ thống**

1. Các vùng mạng trong hệ thống

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **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 |
| 3 | Vùng DMZ | Có | Đặt máy chủ như Reverse Proxy, các giải pháp bảo mật WAF, Email Security Gateway để bảo vệ các ứng dụng khi các ứng dụng này cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet. |
| 4 | Vùng máy chủ nội bộ | Có | Vùng đặt máy chủ nội bộ như máy chủ cơ sở dữ liệu, máy chủ lưu trữ dữ liệu nội bộ… |

1. Phương án bảo đảm an toàn thông tin

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn | Có | Thiết lập cấu hình VPN trên tường lửa Firewall01 cho phép người vận hành, người sử dụng quản lý truy cập, quản trị hệ thống từ xa an toàn. |
| 2 | Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập | Có | Thiết lập cấu hình chức năng IDS/IPS trên các luật/các giao diện của tường lửa Firewall 01 để quản lý truy cập và phòng, chống xâm nhập giữa vùng mạng LAN, DMZ, Máy chủ nội bộ và mạng biên. |
| 3 | Phương án phòng chống mã độc cho máy chủ và máy trạm | Có | Cài đặt phần mềm phòng, chống mã độc cho toàn bộ máy chủ/máy trạm có trong hệ thống sử dụng giải pháp AV (hoặc EDR) |
| 4 | Phương án phòng chống tấn công mạng cho ứng dụng web |  | Sử dụng sản phẩm Tường lửa ứng dụng web WAF01 được đặt tại phân vùng mạng DMZ |
| 5 | Phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử (đối với hệ thống thư điện tử) |  | NA |
| 6 | Phương án dự phòng cho các thiết bị mạng chính | Có | Thiết bị mạng chính bảo gồm Firewall01 và WAF01. Các thiết bị này khi xảy ra sự cố sẽ triển khai giải pháp mã nguồn mở Pfsense và ModSecurity để thay thế tạm thời. |

**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 | Cấu hình trên Firewall01 chỉ cho phép người quản trị, người sử dụng truy cập vào các tài nguyên hệ thống thông qua kết nối VPN. |
| 2 | Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài | Có | Tường lửa Firewall01 cấu hình chỉ cho phép mở cổng 80,443 truy cập từ bên ngoài vào máy chủ ứng dụng web. |
| 3 | Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng. | Có | Thiết lập giới hạn thời gian chờ (timeout) trên Tường lửa Firewall01 để ngắt phiên kết nối VPN khi người dùng không thao tác sử dụng trong 05 phút. |

**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 |  | Tường lửa Firewall01 thiết lập chính sách chỉ cho phép truy cập ra bên ngoài với các dịch vụ phổ biến, phục vụ hoạt động nghiệp vụ bao gồm: TCP 80,443,25,587,…;UDP 53, 123,… |

**1.3.a. Nhật ký hệ thống**

|  |  |  |
| --- | --- | --- |
| **Yêu cầu** | Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống | Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian |
|  |
| **Thiết bị** |
| Router outsite/ | + | + |
| Firewall01/ Checkpoint 12600 | + | + |
| SWDMZ/Cisco2960 | + | + |
| SWSF/ Cisco2960 | + | + |
| SW/Cisco2960 | + | + |
| SW L2/Cisco2960 | + | + |
| WAF/WAF v2secure | + | + |

**1.3.b. Phòng chống xâm nhập**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Yêu cầu** | **P/A** | **Ghi chú/Mô tả** |
| 1 | Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống | Đáp ứng | Sử dụng Tường lửa Firewall01 có tích hợp chức năng IPS để bảo vệ các vùng mạng trong hệ thống. Tính năng IPS được cấu hình trên Firewall01 kiểm soát truy cập và phòng chống xâm nhập giữa các phân vùng mạng nội bộ, máy chủ nội bộ và phân vùng mạng DMZ. |
| 2 | Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng | Đáp ứng | Thực hiện định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng trên Tường lửa Firewall01. |

**1.3.c. Bảo vệ thiết bị hệ thống**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yêu cầu** | Cấu hình  chức năng xác thực trên các thiết bị | Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa | Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa |
| **Thiết bị** |
| Router outsite/ | + | + | + |
| Firewall01/Checkpoint 12600 | + | + | + |
| SWDMZ/Cisco2960 | + | + | + |
| SWSF/ Cisco2960 | + | + | + |
| SW/Cisco2960 | + | + | + |
| SWL2/Cisco2960 | + | + | + |
| WAF/WAF v2secure | + | + | + |