Số: 823/SNgV-VP
Thời gian ký: 01/10/2021 07:46:28 +07:00

UBND TỈNH BÌNH ĐỊNH
SỞ NGOẠI VỤ

TÀI LIỆU THUYẾT MINH HỒ SƠ ĐỀ XUẤT CẤP ĐỘ CHO HỆ THỐNG THÔNG TIN SỞ NGOẠI VỤ

Bình Định, năm 2021

PHẦN I
THUYẾT MINH TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

1. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: Sở Ngoại vụ tỉnh Bình Định

- Số Quyết định thành lập: 195/QĐ-UBND ngày 18/4/2012

- Số Quyết định quy định chức năng, nhiệm vụ và quyền hạn: 3830/QĐ-UBND ngày 27/10/2015

- Người đại diện: Ông Nguyễn Thái Bình

- Chức vụ: Giám đốc Sở

- Địa chỉ: 59-61 Lê Hồng Phong, TP. Quy Nhơn, tỉnh Bình Định

- Thông tin liên hệ:

Số điện thoại: 0256.3820202 Email: vp@songoaivu.binhdinh.gov.vn

2. Thông tin Đơn vị vận hành

2.1. Tên Đơn vị vận hành: Sở Ngoại vụ tỉnh Bình Định

- Số Quyết định thành lập: 195/QĐ-UBND ngày 18/4/2012

- Số Quyết định quy định chức năng, nhiệm vụ và quyền hạn: 3830/QĐ-UBND ngày 27/10/2015

- Người đại diện: Ông Nguyễn Thái Bình

- Chức vụ: Giám đốc Sở

- Địa chỉ: 59-61 Lê Hồng Phong, TP. Quy Nhơn, tỉnh Bình Định

- Thông tin liên hệ:

Số điện thoại: 0256.3820202 Email: vp@songoaivu.binhdinh.gov.vn

2.2. Tên Đơn vị vận hành: Trung tâm Công nghệ thông tin và Truyền thông thuộc Sở Thông tin và Truyền thông Bình Định

- Số Quyết định thành lập: 749/ QĐ-UBND ngày 09/3/2017

- Người đại diện: Ông Nguyễn Văn Bình

- Chức vụ: Giám đốc

- Địa chỉ: 38 Trường Chinh, TP. Quy Nhơn, tỉnh Bình Định

Số điện thoại: 0256.3811626 Email: binhnv@stttt.binhdinh.gov.vn

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của hệ thống: Hệ thống thông tin Sở Ngoại vụ được thiết lập để phục vụ công tác chỉ đạo điều hành, cung cấp thông tin và cung cấp dịch vụ công trực tuyến của Sở Ngoại vụ.

- Đối tượng phục vụ của hệ thống:

+ Toàn thể công chức và người lao động của Sở

+ Các tổ chức, doanh nghiệp, người dân muốn khai thác thông tin trên trang thông tin điện tử của Sở.

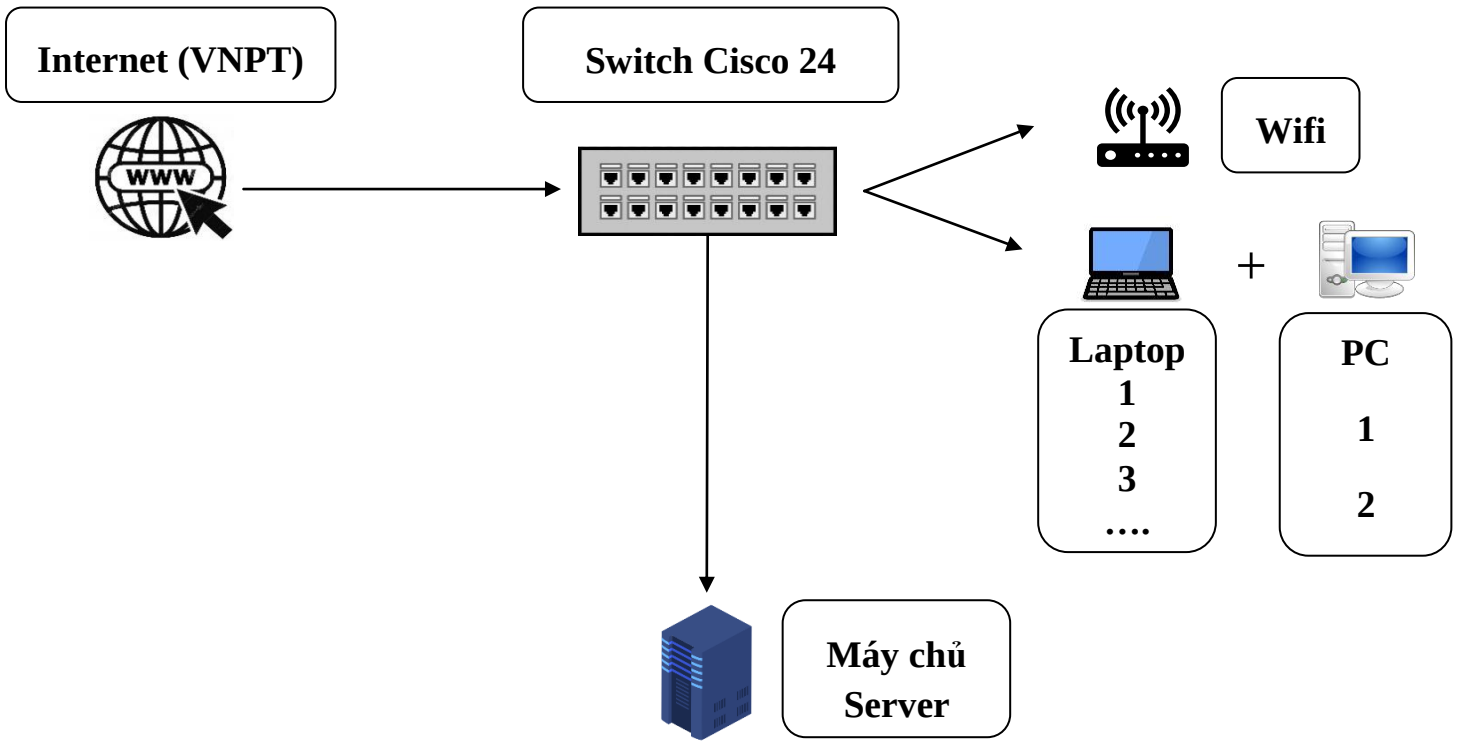
- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi hệ thống Sở Ngoại vụ:

+ Hệ thống Trang thông tin điện tử.

+ Hệ thống mạng nội bộ - LAN của cơ quan.

4. Mô tả cấu trúc của hệ thống

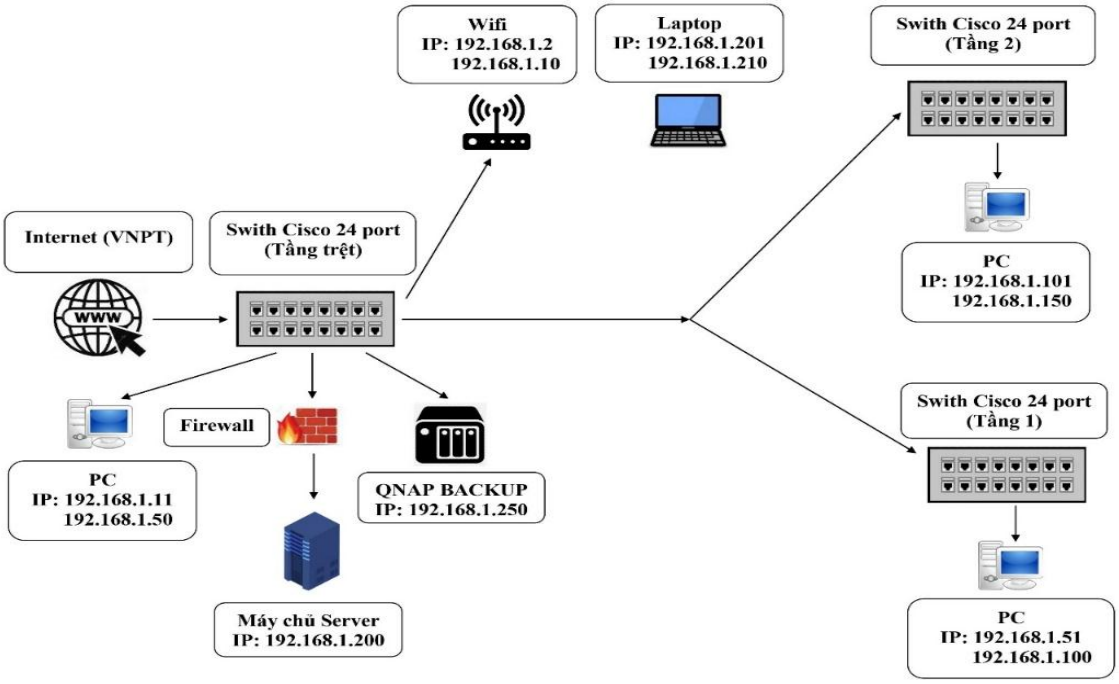
a) Sơ đồ logic tổng thể



Hình 1: Sơ đồ logic tổng thể hệ thống mạng

Các kết nối của thiết bị cùng chung một vùng mạng LAN. Kết nối của các PC và Server trực tiếp đến Switch, kết nối của Switch trực tiếp đến thiết bị Router. Thiết bị Router kết nối đến nhà cung cấp dịch vụ Internet (VNPT).

b) Sơ đồ kết nối vật lý



Hình 2: Sơ đồ kết nối vật lý tổng thể hệ thống mạng

c) Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Router Draytek (Vigor 2912F)	Văn phòng Sở (tầng trệt)	Kết nối đến Internet; và định tuyến động với các Router của 02 ISP
2	Switch 24 port TP-Link	Đặt tại các đầu mối các tầng	Bộ chia kết nối có dây, truyền tín hiệu đến các thiết bị khác
3	Switch 8 port TP-Link Switch 5 port TP-Link Igate	Đặt tại các phòng chuyên môn thuộc Sở, Phòng họp	Bộ chia kết nối có dây, truyền tín hiệu đến các thiết bị khác
4	Wireless Access point	Tầng trệt: 02 Tầng 1: 03 Tầng 2: 01	Nhận tín hiệu dây từ Router, phát không dây tín hiệu Internet cho các thiết bị dùng wireless

d) Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

STT	Tên dịch vụ	Máy chủ triển khai	Mục đích sử dụng
1	Trang thông tin điện tử của Sở Ngoại vụ	Hosting tại máy chủ của cơ quan/	Cung cấp tin tức và các dịch vụ giải quyết TTHC bên trong hệ thống và cung cấp thông tin công khai về DVCTT, tình trạng giải quyết TTHC cho người sử dụng bên ngoài Internet
2	Hệ thống mạng nội bộ- LAN của cơ quan	Ngang hàng	Các máy tính cá nhân được kết nối với nhau tạo nên mạng LAN để chia sẻ tài nguyên mạng, chia sẻ máy in mạng

PHẦN II

THUYẾT MINH ĐỀ XUẤT CẤP ĐỘ AN TOÀN HỆ THỐNG THÔNG TIN

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

Căn cứ Điều 8 Nghị định số 85/2016/NĐ-CP ngày 01/7/2017 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ, Hệ thống thông tin Sở Ngoại vụ là hệ thống cơ sở hạ tầng thông tin thuê dịch vụ và hệ thống mạng nội bộ.

STT	Hệ thống	Loại thông tin xử lý	Loại hình HTTT	Cấp độ đề xuất	Căn cứ đề xuất
1	Trang thông tin điện tử của Sở Ngoại vụ	Trang riêng	Hệ thống thông tin phục vụ hoạt động nội bộ trong phạm vi ngành; hoặc người dân, doanh nghiệp quan tâm đến thông tin đăng trên web của Sở và TTHC do Sở cung cấp	2	Điểm a, Khoản 2, Điều 8 Nghị định số 85/2016/NĐ-CP
2	Hệ thống mạng nội bộ - LAN của cơ quan	Ngang hàng	Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của cơ quan	2	Khoản 3, Điều 8 Nghị định số 85/2016/NĐ-CP

2. Thuyết minh chi tiết đối với hệ thống thông tin

- Trang thông tin điện tử: Cung cấp thông tin hoạt động chuyên ngành của Sở đến với người dân, tổ chức, doanh nghiệp; Cung cấp các dịch vụ hành chính công; Cung cấp thông tin chỉ đạo điều hành của lãnh đạo Sở; văn bản pháp luật.

- Hệ thống mạng nội bộ (LAN) của cơ quan: Hệ thống phần cứng và cáp kết nối đảm bảo truyền tải thông tin giữa các hệ thống và thiết bị bên trong và bên ngoài mạng LAN. Sở Ngoại vụ tiến hành xây dựng phương án đảm bảo an toàn hệ thống thông tin đối với hệ thống này như phần III.

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

1. Yêu cầu quản lý

1.1. Mục tiêu, nguyên tắc bảo đảm an toàn thông tin

*** Mục tiêu**

Đảm bảo an toàn thông tin là làm cho hệ thống hoạt động thông suốt và không bị tấn công bởi virus và hacker làm mất dữ liệu cũng như gián đoạn quá trình hoạt động của hệ thống.

* **Nguyên tắc**

- Cài đặt và cập nhật các phần mềm diệt virus cho máy chủ và các máy con.

- Định kỳ kiểm tra thông tin truy cập của hệ thống, kiểm soát băng thông đường truyền.

- Rà soát và thay đổi các tài khoản, các ứng dụng.

- Hạn chế truy cập vào các website không rõ nguồn gốc.

- Trang bị cho các máy tính để bàn, máy tính xách tay và máy chủ phần mềm diệt virus.

- Tăng cường trao đổi thông tin qua hệ thống hộp thư điện tử công vụ và văn phòng điện tử (hạn chế sử dụng USB, thẻ nhớ, các thiết bị gắn trực tiếp vào máy tính).

1.2. Trách nhiệm bảo đảm an toàn thông tin

- Các cán bộ làm về an toàn thông tin, người sử dụng đầu cuối, các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin.

- Người đứng đầu cơ quan chỉ đạo thực hiện việc kiểm tra về vấn đề an toàn thông tin.

- Cán bộ chuyên trách công nghệ thông tin thường xuyên kiểm tra mức độ an toàn của hệ thống.

- Người sử dụng các dịch vụ do máy chủ cung cấp có trách nhiệm bảo mật thông tin của mình.

1.3. Phạm vi chính sách an toàn thông tin

Các văn bản, chính sách quản lý hệ thống thông tin trong phạm vi cơ quan

- Kế hoạch Ứng dụng CNTT hằng năm.

- Quyết định số 16/QĐ-SNgV ngày 05/9/2013 về Quy chế hoạt động Trang thông tin điện tử của Sở Ngoại vụ tỉnh Bình Định;

- Quy chế hoạt động của Ban Biên tập Website Sở Ngoại vụ tỉnh Bình Định;

- Quyết định số 29/QĐ-SNgV ngày 09/12/2013 về Quy chế hoạt động của Ban Biên tập Website Sở Ngoại vụ tỉnh Bình Định;

- Quyết định số 816/QĐ-SNgV ngày 24/10/2014 về Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động nội bộ của Sở Ngoại vụ tỉnh Bình Định;

- Quyết định số 817/QĐ-SNgV ngày 24/10/2014 về Quy chế quản lý, sử dụng thư điện tử công vụ trong hoạt động của Sở Ngoại vụ tỉnh Bình Định;

- Quyết định số 1048/QĐ-SNgV ngày 22/11/2016 về Quy chế quản lý, sử dụng Phần mềm chuyển, nhận văn bản hành chính giữa Bộ Ngoại giao và Sở Ngoại vụ tỉnh Bình Định;

- Quyết định số 1279/QĐ-SNgV ngày 28/12/2018 về Quy chế quản lý và sử dụng Văn phòng điện tử liên thông của Sở Ngoại vụ tỉnh Bình Định.

- Quyết định số 816/QĐ-SNgV ngày 30/9/2021 về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động UDCNTT của Sở Ngoại vụ tỉnh Bình Định;

1.4. Tổ chức bảo đảm an toàn thông tin

- 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 hổng bảo mật.

1.5. Bảo đảm nguồn nhân lực

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

1.6. Quản lý vận hành hệ thống

- Việc quản lý vận hành hệ thống như: Quản lý an toàn máy chủ, an toàn ứng dụng, an toàn dữ liệu, an toàn mạng, sự cố an toàn thông tin, an toàn người sử dụng đầu cuối của các hệ thống thông tin thành phần tại Sở đều được kiểm tra đảm bảo các hệ thống thông tin hoạt động ổn định 24/24, có đầy đủ các thiết bị bảo mật, an toàn và lưu trữ dữ liệu thường xuyên.

- Các quy định như xây dựng kế hoạch, chính sách, quy trình thực hiện quản lý an toàn hạ tầng mạng được đơn vị cho thuê dịch vụ thực hiện.

- Hệ thống mạng nội bộ- LAN của cơ quan luôn được theo dõi, quản lý đảm bảo hoạt động thông suốt, các máy tính được trang bị phần mềm diệt virus.

2. Yêu cầu kỹ thuật

2.1. Bảo đảm an toàn mạng *(cấp độ 2 trở lên)*

- Thường xuyên phối hợp với đơn vị cho thuê dịch vụ để vận hành hệ thống ổn định;

- Công chức phụ trách công nghệ thông tin tại cơ quan phải thường xuyên nghiên cứu, cập nhật các kiến thức về an toàn, an ninh thông tin, nguy cơ tiềm ẩn có thể gây mất thông tin và các biện pháp phòng tránh khi tiến hành các hoạt động quản lý hay kỹ thuật nghiệp vụ;

- Thường xuyên thực hiện việc theo dõi bảng ghi nhật ký hệ thống (logfile) và các sự kiện khác có liên quan để đánh giá, báo cáo các rủi ro và mức độ nghiêm trọng các rủi ro đó. Các rủi ro đó có thể xảy ra do sự truy cập trái phép, sử dụng trái phép, mất, thay đổi hoặc phá hủy thông tin và hệ thống thông tin;

- Khi thiết lập các dịch vụ trên môi trường mạng Internet, chỉ cung cấp những chức năng thiết yếu bảo đảm duy trì hoạt động của hệ thống thông tin; hạn

chế sử dụng chức năng, cổng giao tiếp mạng, giao thức và các dịch vụ không cần thiết.

2.2. Bảo đảm an toàn ứng dụng

- Thực hiện cấp phát, thu hồi, cập nhật và quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của sở; hướng dẫn người dùng thay đổi mật khẩu cá nhân theo quy định.

- Nghiêm chỉnh chấp hành các quy định nội bộ về an toàn thông tin của cơ quan, đơn vị và các quy định khác của pháp luật.

- Thường xuyên cài đặt và cập nhật các phần mềm diệt virus,.. cho tất cả các máy tính cá nhân, máy tính xách tay.

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

- Thiết lập chính sách lưu dự phòng dữ liệu định kỳ.

2.3. Bảo đảm an toàn dữ liệu

- Hệ thống mạng nội bộ của Sở được thiết kế, xây dựng theo mô hình nhóm (Group) cho từng phòng và cấp địa chỉ mạng cố định cho từng cá nhân, cho từng máy tính của cơ quan và giao các đơn vị, phòng chuyên môn quản lý, theo dõi nhằm mục đích quản lý hệ thống chặt chẽ, an toàn và bảo mật.

- Định kỳ lưu trữ dữ liệu vào các thiết bị lưu trữ như Qnap, các server./.