UBND TỈNH GIA LAI
SỞ CÔNG THƯƠNG

Số: 1496/SCT-VP
V/v đề nghị thẩm định và phê duyệt hồ sơ đề xuất cấp độ an toàn HTTT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Gia Lai, ngày 06 tháng 12 năm 2018

Kính gửi: Sở Thông tin và Truyền thông.

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính Phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Công văn số 1202/STTTT-CNTT ngày 19/11/2018 của Sở Thông tin và Truyền thông về việc hướng dẫn thực hiện công tác xác định cấp độ an toàn thông tin. Sau khi xây dựng hồ sơ, Sở Công Thương đề nghị Sở Thông tin và Truyền thông thẩm định hồ sơ đề xuất cấp độ an toàn hệ thống thông tin cụ thể như sau:

Phần 1. Thông tin chung

1. Tên hệ thống thông tin: Sở Công Thương.

2. Đơn vị vận hành hệ thống thông tin: Sở Công Thương.

3. Địa chỉ: Tầng 7, 8 trụ sở liên cơ quan, 17 Trần Hưng Đạo, phường Tây Sơn, thành phố Pleiku, tỉnh Gia Lai.

4. Cấp độ an toàn hệ thống thông tin đề xuất: Cấp độ 2.

Phần 2. Hồ sơ kèm theo

1. Tài liệu thuyết minh Hồ sơ đề xuất cấp độ gửi kèm theo bao gồm: Thuyết minh tổng quan về hệ thống thông tin; Thuyết minh về việc đề xuất cấp độ căn cứ trên các tiêu chí theo quy định của pháp luật; Thuyết minh phương án bảo đảm an toàn thông tin theo cấp độ tương ứng.

2. Tài liệu thiết kế hệ thống.

Sở Công Thương kính đề nghị Sở Thông tin và Truyền thông xem xét thẩm định và trình cấp có thẩm quyền phê duyệt./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở;
- TT KC&XTTM;
- Phòng QLXNK;
- Lưu: VT, VP.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

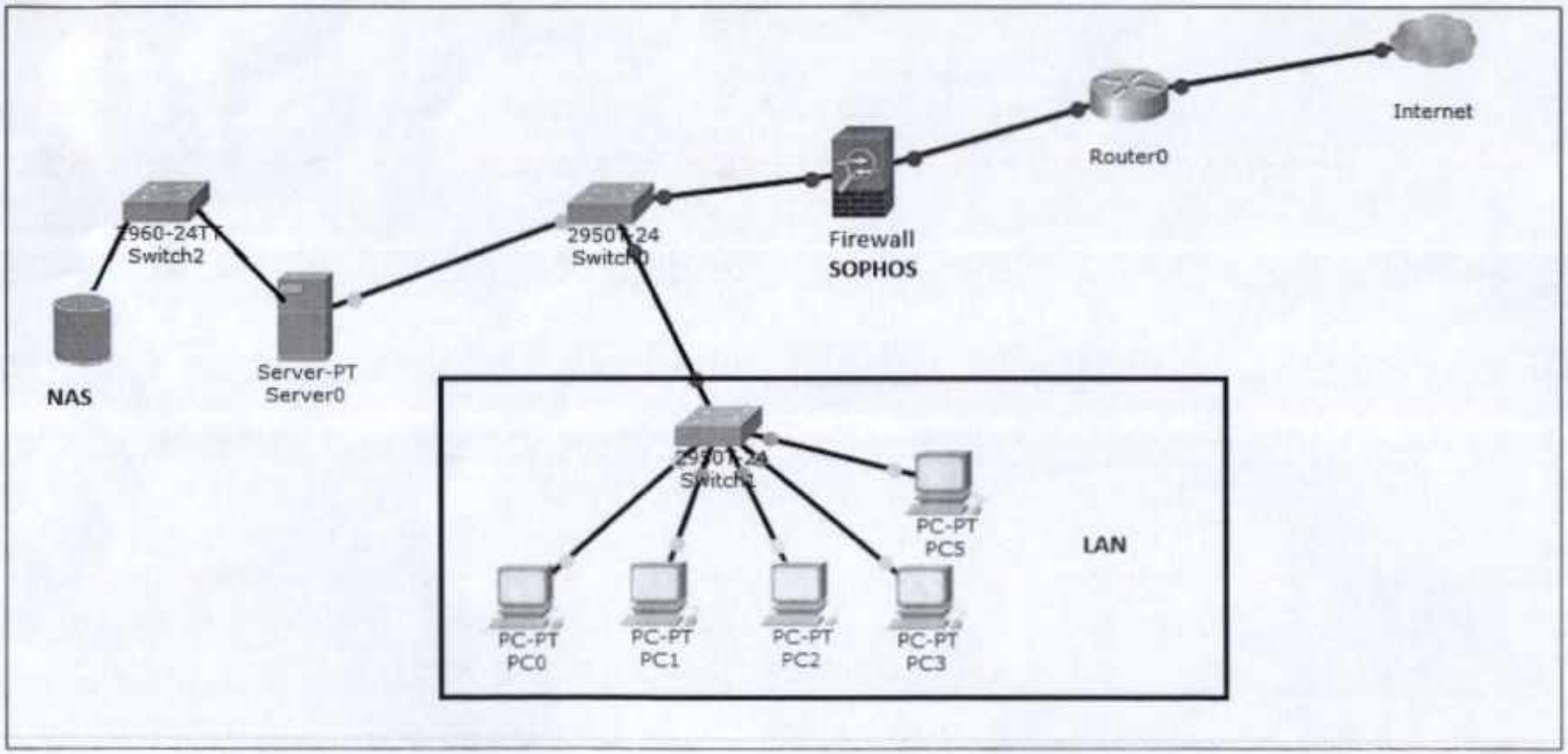
SỞ CÔNG THƯƠNG TỈNH GIA LAI

Đào Thị Thu Nguyệt

UBND TỈNH GIA LAI
SỞ CÔNG THƯƠNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

SƠ ĐỒ THIẾT KẾ HỆ THỐNG TẠI SỞ CÔNG THƯƠNG



UBND TỈNH GIA LAI
SỞ CÔNG THƯƠNG

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

Gia Lai - 2018

PHẦN I
THUYẾT MINH TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

1. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: Sở Thông tin và Truyền Thông

- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn:

+ Quyết định số 127/QĐ-UBND ngày 07/4/2008 của UBND tỉnh Gia Lai.

+ Thông tư liên tịch số 06/2016/TTLT-BTTTT-BNV ngày 10/3/2016 của Liên Bộ Thông tin và Truyền thông và Bộ Nội vụ và các quy định pháp luật khác có liên quan.

- Người đại diện: Nguyễn Ngọc Hùng –Giám đốc Sở Thông tin và Truyền thông.

- Địa chỉ: Trụ sở liên cơ quan, 17 Trần Hưng Đạo, phường Tây Sơn, Tp.Pleiku, tỉnh Gia Lai.

- Thông tin liên hệ:

2. Thông tin Đơn vị vận hành

- Tên Tổ chức: Sở Công Thương

- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn:

+ Quyết định số 36/2015/QĐ-UBND ngày 04/12/2015 của Ủy ban nhân dân tỉnh Gia Lai quy định chức năng, nhiệm vụ, quyền hạn, cơ cấu tổ chức của Sở Công Thương tỉnh Gia Lai;

+ Thông tư liên tịch số 22/2015/TTLT-BCT-BNV ngày 30/6/2015 của Bộ Công Thương, Bộ Nội vụ hướng dẫn chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của cơ quan chuyên môn về công thương thuộc Ủy ban nhân dân cấp tỉnh, cấp huyện và theo hướng dẫn của cơ quan chức năng cấp trên.

- Người đại diện: Bùi Khắc Quang – Tỉnh ủy viên, Giám đốc Sở Công Thương.

- Địa chỉ: Tầng 7,8 Trụ sở liên cơ quan, 17 Trần Hưng Đạo, phường Tây Sơn, Tp.Pleiku, tỉnh Gia Lai.

- Thông tin liên hệ: 02693.824.354, thư điện tử: sct@gialai.gov.vn

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của hệ thống: Hệ thống thông tin Sở Công Thương 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.

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

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

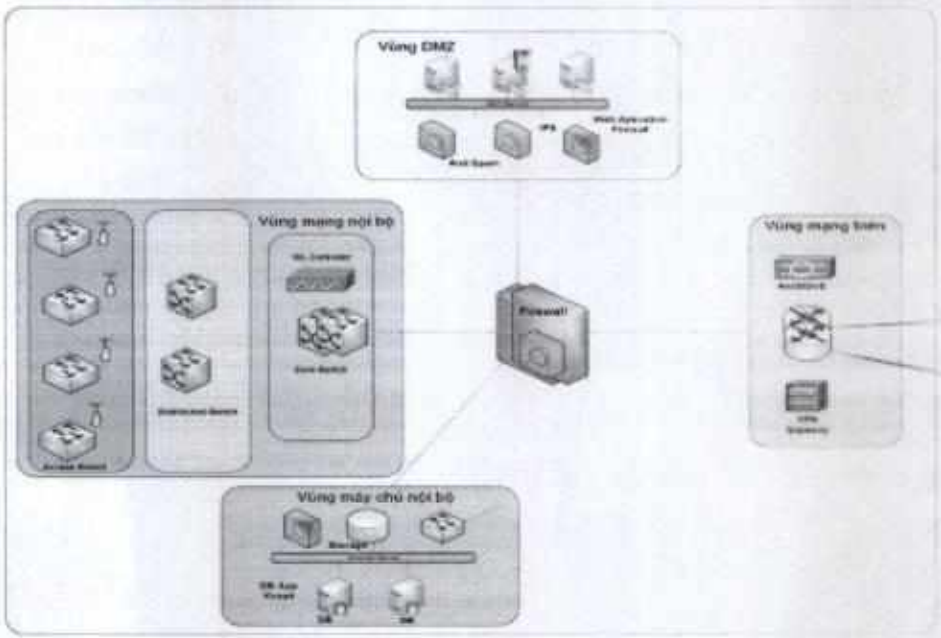
+ Hệ thống Quản lý văn bản và điều hành.

+ Hệ thống thông tin một cửa điện tử

+ Hệ thống Trang thông tin điện tử.

4. Mô tả cấu trúc của hệ thống

a) Sơ đồ logic tổng thể



Hình 1: Cấu trúc logic của hệ thống A

Các vùng mạng được thiết kế như sau:

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

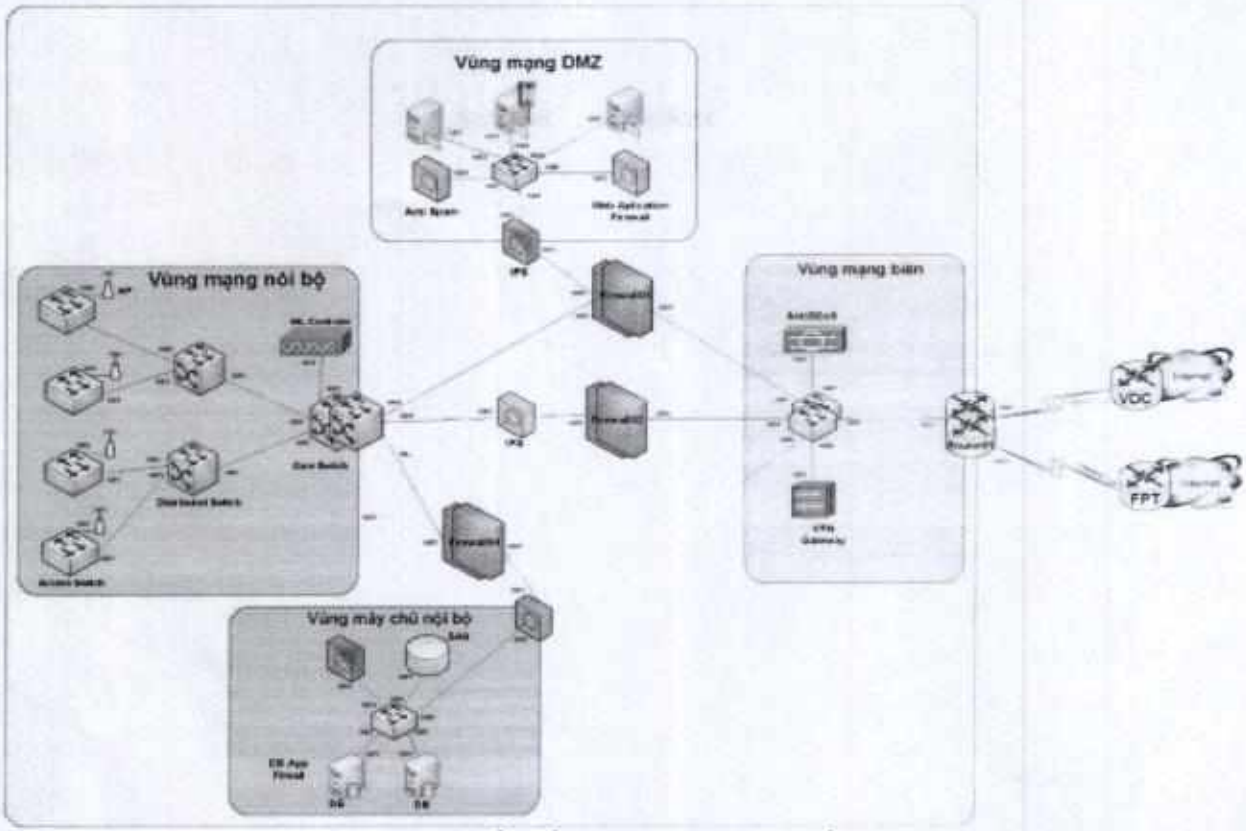
+ Vùng DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị Anti-Spam.

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

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

+ Vùng mạng nội bộ đặt các máy tính của người sử dụng.

b) Sơ đồ kết nối vật lý



Hình 2: Kết nối vật lý của Hệ thống A

b) *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	Vùng mạng biên	Kết nối và định tuyến
2	Firewall/SOPHOS	Vùng DMZ	Quản lý truy cập và bảo vệ vùng mạng LAN

c) 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	Hệ thống quản lý văn bản và điều hành	Máy chủ /WindowServer 2012	Cung cấp ứng dụng quản lý văn bản cho cán bộ bên trong hệ thống; kết nối, liên thông với các hệ thống liên quan.
2	Hệ thống thông tin một cửa điện tử, Dịch vụ công trực tuyến	Máy chủ /WindowServer 2012	Cung cấp ứng dụng theo dõi, quản lý thông tin tiếp nhận, 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
3	Trang thông tin điện tử của cơ quan	Máy chủ /WindowServer 2012	Hệ thống thông tin phục vụ người dân, doanh nghiệp, cung cấp thông tin và DVC.

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

Hệ thống thông tin thuộc phạm vi quản lý của Công Thương bao gồm các hệ thống thông tin với cấp độ đề xuất tương ứng, bao gồm:

STT	Hệ thống	Loại thông tin xử lý	Loại hình HTTT	Cấp độ đề xuất	Căn cứ đề xuất
1	Phòng máy chủ		Hệ thống cơ sở hạ tầng thông tin dùng chung phục vụ hoạt động của một cơ quan, tổ chức.	1	Phòng máy chủ/Trung tâm tích hợp dữ liệu của cơ quan, đơn vị
2	Hệ thống quản lý văn bản và điều hành của Sở	Thông tin riêng của tổ chức	Hệ thống thông tin phục vụ hoạt động nội bộ các cơ quan nhà nước của tỉnh	2	Điểm a Khoản 2, Điều 9Nghị định số 85/2016/NĐ-CP
3	Hệ thống một cửa điện tử của Sở - DVC trực tuyến	Thông tin riêng của tổ chức	Hệ thống thông tin phục vụ hoạt động nội bộ các cơ quan nhà nước của tỉnh	3	Điểm a Khoản 2, Điều 9 Nghị định số 85/2016/NĐ-CP
4	Trang thông tin điện tử của cơ quan	Thông tin công cộng	Hệ thống thông tin phục vụ người dân, doanh nghiệp, cung cấp thông tin và DVC trực tuyến từ mức độ 2 trở xuống	2	Điểm a, Khoản 2, Điều 8Nghị định số 85/2016/NĐ-CP

5	Hệ thống mạng nội bộ - LAN của cơ quan		Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động của cơ quan	2	Khoản 4, Điều 9 Nghị định số 85/2016/NĐ-CP

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

- Các hoạt động ứng dụng CNTT của Sở phải tuân thủ theo nguyên tắc đảm bảo an toàn thông tin được quy định tại Quyết định 2072/QĐ-UBND ngày 16 tháng 10 năm 2014 của UBND tỉnh quy định về đảm bảo an toàn, an ninh thông tin trên môi trường mạng trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Gia Lai.

- Việc thực hiện các phương pháp an toàn thông tin phải tuân theo quy định của Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về việc đảm bảo an toàn hệ thống thông tin theo cấp độ và quy định của pháp luật có liên quan.

1.2. Trách nhiệm của 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

- Trách nhiệm của cán bộ chuyên trách Công nghệ thông tin:

+ Thực hiện quản lý tất cả các tài khoản truy cập vào hệ thống thông tin của đơn vị; hướng dẫn người sử dụng thay đổi mật khẩu.

+ Triển khai, áp dụng các giải pháp đảm bảo an toàn thông tin mạng trong toàn hệ thống; triển khai các giải pháp phòng chống virus, mã độc, có giải pháp chống truy cập trái phép vào hệ thống thông tin.

+ Quản lý thiết bị công nghệ thông tin lưu trữ các thông tin thuộc danh mục bí mật nhà nước.

+ Thường xuyên sao lưu dữ liệu.

+ Thường xuyên thực hiện phân tích, đánh giá và báo cáo các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin đối với hệ thống thông tin của đơn vị; nguyên nhân gây ra các rủi ro và nguy cơ gây mất an toàn, an ninh thông tin mạng.

- Trách nhiệm của công chức, viên chức tham gia sử dụng và khai thác hệ thống thông tin:

+ Thường xuyên cập nhật và thực hiện hướng dẫn về an toàn thông tin của cán bộ phụ trách;

+ Không được mở các thư điện tử, các tập tin có nguồn gốc không rõ ràng;

+ Đặt mật khẩu truy nhập vào máy tính, thường xuyên thay đổi mật khẩu máy tính;

1.3. Phạm vi chính sách an toàn thông tin

Quy định bảo đảm an toàn thông tin mạng, bao gồm: Bảo vệ thông tin cá nhân; bảo vệ hệ thống thông tin mạng; giám sát an toàn hệ thống thông tin; đảm bảo an toàn thông tin nội bộ; quy trình ứng cứu, khắc phục sự cố mạng; quản lý và sử dụng thiết bị soạn thảo, lưu trữ văn bản mật của cơ quan.

1.4. Tổ chức bảo đảm an toàn thông tin

- Trung tâm Công nghệ thông tin thuộc Sở Thông tin truyền thông là đơn vị bảo đảm an toàn thông tin cho Sở.

- Là đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền về quản lý an toàn thông tin; trong công tác hỗ trợ điều phối xử lý sự cố an toàn thông tin

1.5. Bảo đảm nguồn nhân lực

- 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

- Có ban hành quy chế về đảm bảo an toàn thông tin trong hoạt động của Sở

- Tổ chức tuyên truyền, phổ biến nâng cao nhận thức về an toàn thông tin cho công chức, viên chức.

- Cử công chức, viên chức phụ trách Công nghệ thông tin tham gia đầy đủ các lớp đào tạo vệ an toàn thông tin.

1.6. Quản lý thiết kế, xây dựng hệ thống.

- Thiết kế an toàn hệ thống thông tin: Tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin; mô tả thiết kế và các thành phần hệ thống thông tin; tài liệu mô tả phương án đảm bảo an toàn thông tin theo cấp độ; Tài liệu mô tả phương án lựa chọn giải pháp công nghệ đảm bảo an toàn thông tin.

- Phát triển phần mềm thuê khoán: Có hợp đồng, biên bản và các cam kết đối với bên thuê khoán các nội dung liên quan đến việc phát triển phần mềm thuê khoán; yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm; Các phần mềm trước khi đưa vào sử dụng đều được kiểm thử trước khi vận hành khai thác,

- Thử nghiệm và nghiệm thu hệ thống: Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng; có quy trình thử nghiệm và nghiệm thu hệ thống.

1.7. Quản lý vận hành hệ thống

- Quản lý an toàn máy chủ và ứng dụng: Có chính sách, quy trình quản lý an toàn máy chủ và dịch vụ; quản lý truy cập mạng của máy chủ; quản lý truy cập và quản trị máy chủ và ứng dụng.

- Quản lý an toàn dữ liệu: Có chính sách, quy trình dự phòng và khôi phục dữ liệu; thực hiện quy trình sao lưu, tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu, dữ liệu..

- Quản lý an toàn mạng: Có chính sách, quy trình quản lý an toàn mạng gồm: quản lý, vận hành hoạt động bình thường của hệ thống; cập nhật sao lưu dự phòng các tập tin cấu hình hệ thống và khôi phục hệ thống sau khi xảy ra sự cố.

- Quản lý sự cố an toàn thông tin: Có chính sách, quy trình quản lý sự cố an toàn thông tin bao gồm: Phân nhóm sự cố; phát hiện, phân loại và xử lý sự cố an toàn thông tin mạng; quy trình ứng cứu sự cố mạng thông thường; nghiêm trọng và cơ chế phối hợp với cơ quan chức năng, các nhóm chuyên gia, hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin.

- Quản lý an toàn người sử dụng đầu cuối: Có chính sách, quy tình quản lý an toàn người sử dụng đầu cuối bao gồm: quản lý truy cập, sử dụng tài nguyên nội bộ, quản lý truy cập mạng và tài nguyên Internet.

1.8. Kiểm tra, đánh giá và quản lý rủi ro: Định kỳ thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin theo quy định của pháp luật.

2. Yêu cầu kỹ thuật

2.1. Bảo đảm an toàn mạng

a) Thiết kế hệ thống: Hệ thống gồm các vùng mạng sau: Vùng mạng nội bộ, vùng mạng biên, vùng DMZ, vùng máy chủ nội bộ.

b) Kiểm soát truy cập từ bên ngoài mạng: 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; kiểm soát truy cập bên ngoài vào hệ thống; Thiết lập thời gian chờ để đóng phiên kết nối khi hệ thống ko nhận được yêu cầu từ người dùng.

c) Kiểm soát truy cập từ bên trong mạng: Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ.

d) Nhật ký hệ thống: Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống.

e) Phòng chống xâm nhập: Phòng chóng xâm nhập bảo vệ vùng máy chủ và mạng nội bộ.

f) Phòng chống phần mềm độc hại trên môi trường mạng: Xây dựng phương án sử dụng phần mềm phòng, chống mã độc trên máy chủ và có cơ chế tự động cập nhật phiên bản mới hoặc dấu hiệu nhận dạng mã độc mới cho phần mềm này.

g) Bảo vệ thiết bị hệ thống: Thiết lập cấu hình cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa.

2.2. Bảo đảm an toàn máy chủ

a) Xác thực: Có cơ chế xác thực bằng mật khẩu bảo đảm độ phức tạp cần thiết (mật khẩu gồm số, chữ cái, ký tự đặc biệt); yêu cầu thay đổi mật khẩu định kỳ theo quy định; vô hiệu hóa các tài khoản mặc định hoặc không hoạt động trên hệ thống; vô hiệu hóa các dịch vụ, phần mềm không sử dụng trên máy chủ.

b) Kiểm soát truy cập: Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa.

c) Nhật ký hệ thống: Ghi nhật ký thông tin kết nối mạng tới máy chủ, thông tin đăng nhập máy chủ; lỗi phát sinh trong quá trình hoạt động; thông tin thay đổi cấu hình máy chủ…

d) Phòng chống xâm nhập: Loại bỏ các tài khoản không sử dụng trên máy chủ; Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ; thường xuyên cập nhật các bản vá , xử lý các điểm yếu an toàn cho hệ điều hành và các dịch vụ hệ thống trên máy chủ.

e) Phòng chống phần mềm độc hại: Cài đặt các phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; Thường xuyên kiểm tra, dò quét và xử lý các phần mềm độc hại trước khi cài đặt.

f) Xử lý máy chủ khi chuyển giao: Xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.

2.3. Bảo đảm an toàn ứng dụng

a) Xác thực: Thiết lập cấu hình ứng dụng xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng; Yêu cầu thay đổi mật khẩu mặc định; Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ và hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định.

b) Kiểm soát truy cập: Chỉ cho phép sử dụng các kết nối an toàn khi truy cập, quản trị ứng dụng thời xa.

c) Nhật ký hệ thống: Ghi nhật ký các thông tin truy cập ứng dụng; Thông tin đăng nhập quản trị ứng dụng; thông tin các lỗi phát sinh trong quá trình hoạt động; Thông tin thay đổi cấu hình ứng dụng.

d) Bảo mật thông tin liên lạc: Không sử dụng kết nối mạng không mã hóa trong việc quản trị ứng dụng từ xa.

e) Chống chối bỏ: Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng.

2.4. Bảo đảm an toàn dữ liệu

a) Nguyên vẹn dữ liệu: Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống.

b) Bảo mật dữ liệu: Lưu trữ có mã hóa các thông tin, dữ liệu trên phương tiện lưu trữ.

c) Sao lưu dự phòng: Thực hiện sao lưu định kỳ các thông tin dữ liệu cơ bản, tập tin hệ thống, cơ sở dữ liệu, dữ liệu.

Trên đây là tài liệu thuyết minh hồ sơ đề xuất cấp độ cho hệ thống thông tin Sở Công Thương. Kính đề nghị Sở Thông tin và Truyền thông xem xét thẩm định và trình cấp có thẩm quyền phê duyệt./.