

QUYẾT ĐỊNH
Về việc phê duyệt cấp độ an toàn các hệ thống thông tin
hiện đang vận hành tại thị xã An Khê

ỦY BAN NHÂN DÂN THỊ XÃ

Căn cứ Luật Tổ chức Chính quyền địa phương năm 2015; Luật sửa đổi, bổ sung một số điều của luật tổ chức chính phủ và Luật tổ chức chính quyền địa phương năm 2019;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 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 tháng 4 năm 2017 của Bộ trưởng 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 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Xét đề nghị của Trưởng phòng Văn hóa và Thông tin tại Văn bản số 143/PVHTT ngày 16 tháng 4 năm 2021.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt cấp độ an toàn các hệ thống thông tin hiện đang vận hành tại thị xã An Khê, cụ thể như sau:

1. Thông tin chung: Văn phòng HĐND và UBND thị xã là đơn vị vận hành các hệ thống thông tin dùng chung của thị xã An Khê, trong đó có các hệ thống thông tin cấp độ 2, cụ thể:

- Hệ thống Máy chủ thị xã;
- Hệ thống Cổng/Trang thông tin điện tử của thị xã/xã;
- Hệ thống mạng LAN của các cơ quan, đơn vị thị xã.

2. Cấp độ an toàn hệ thống thông tin: Cấp độ 2

3. Phương án bảo đảm an toàn thông tin

a) Phương án đảm bảo an toàn thông tin trong thiết kế hệ thống thông tin tương ứng với cấp độ 2 là phù hợp với quy định tại khoản 2 Điều 9 Thông tư số 03/2017/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

b) Phương án đảm bảo an toàn thông tin trong quá trình vận hành hệ thống

thông tin tương ứng với cấp độ 2 là phù hợp với quy định tại khoản 2 Điều 9 Thông tư số 03/2017/TT-BTTTT và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

Điều 2. Tổ chức thực hiện

Văn phòng HĐND và UBND thị xã có trách nhiệm bảo đảm an toàn các hệ thống thông tin quản lý, đang vận hành theo các quy định tại Điều 22 Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và Tiêu chuẩn quốc gia TCVN 11930:2017 về Công nghệ thông tin - các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

Điều 3. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Chánh Văn phòng HĐND và UBND thị xã, Trưởng phòng Văn hóa và Thông tin thị xã, Thủ trưởng các cơ quan, đơn vị và cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này. /s/

Nơi nhận:

- Như điều 3;
- Sở Thông tin và Truyền thông;
- TT. Thị ủy;
- TT. HĐND thị xã;
- Chủ tịch và các PCT UBND thị xã;
- Các Ủy viên UBND thị xã;
- UBND các xã, phường;
- Cổng thông tin điện tử thị xã;
- Lưu: VT, VHTT. /s/

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**



Nguyễn Hùng Vỹ



ỦY BAN NHÂN DÂN THỊ XÃ AN KHÊ

**TÀI LIỆU THUYẾT MINH HỒ SƠ ĐỀ XUẤT CẤP ĐỘ
CHO HỆ THỐNG THÔNG TIN THỊ XÃ AN KHÊ**

An Khê - 2021

PHẦN I

THUYẾT MINH TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN



1. Thông tin Chủ quản hệ thống thông tin

- Tên Tổ chức: Ủy ban nhân dân thị xã An Khê.
- Quyết định thành lập: Nghị định số 155/2003/NĐ-CP ngày 09/12/2003 về việc thành lập thị xã An Khê và huyện Đak Pơ, thành lập xã Đak Pơ thuộc huyện Đak Pơ, tỉnh Gia Lai.

- Người đại diện: Ông Nguyễn Hùng Vỹ, Chủ tịch Ủy ban nhân dân thị xã.
- Địa chỉ: Số 1356 Quang Trung, phường Tây Sơn, thị xã An Khê, tỉnh Gia Lai.
- Thông tin liên hệ: Số điện thoại 0269 3832277, ubndankhe@gialai.gov.vn.

2. Thông tin Đơn vị vận hành

- Tên Đơn vị vận hành: Văn phòng HĐND và UBND thị xã An Khê, tỉnh Gia Lai.
- Số Quyết định thành lập/Quy định chức năng, nhiệm vụ và quyền hạn:
- Người đại diện: Vũ Thị Tú Trinh - Chánh Văn phòng HĐND và UBND thị xã.
- Địa chỉ: Số 1356 Quang Trung, phường Tây Sơn, thị xã An Khê, tỉnh Gia Lai.
- Thông tin liên hệ: SĐT: 0269 3832 277. Email: trinhvtt.ankhe@gialai.gov.vn.

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của hệ thống: Hệ thống thông tin Thị xã An Khê được thiết lập để phục vụ công tác chỉ đạo điều hành, cung cấp thông tin của thị xã An Khê.

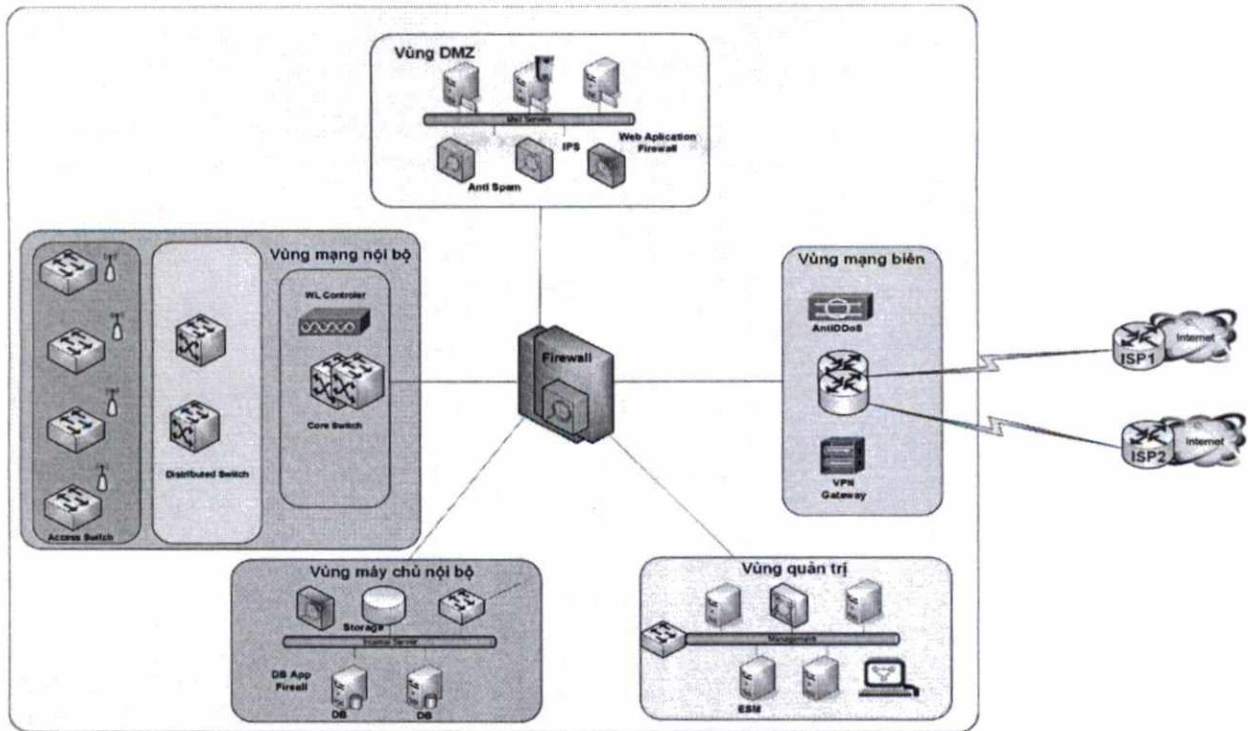
- Đối tượng phục vụ của hệ thống: Cơ quan, tổ chức, doanh nghiệp, người dân trên địa bàn thị xã An Khê.

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

- + Hệ thống máy chủ thị xã;
- + Hệ thống Cổng/Trang thông tin điện tử thị xã/xã;
- + Hệ thống mạng LAN của các cơ quan, đơn vị thị xã.

4. Mô tả cấu trúc của hệ thống

a) Sơ đồ logic tổng thể



Cấu trúc logic của hệ thống thị xã An Khê

Các vùng mạng được thiết kế như sau:

+ Vùng mạng biên được thiết kế để kết nối hệ thống mạng thị xã An Khê ra các mạng bên ngoài và mạng Internet; bảo vệ hệ thống thị xã An Khê 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 (tích hợp trong Firewall).

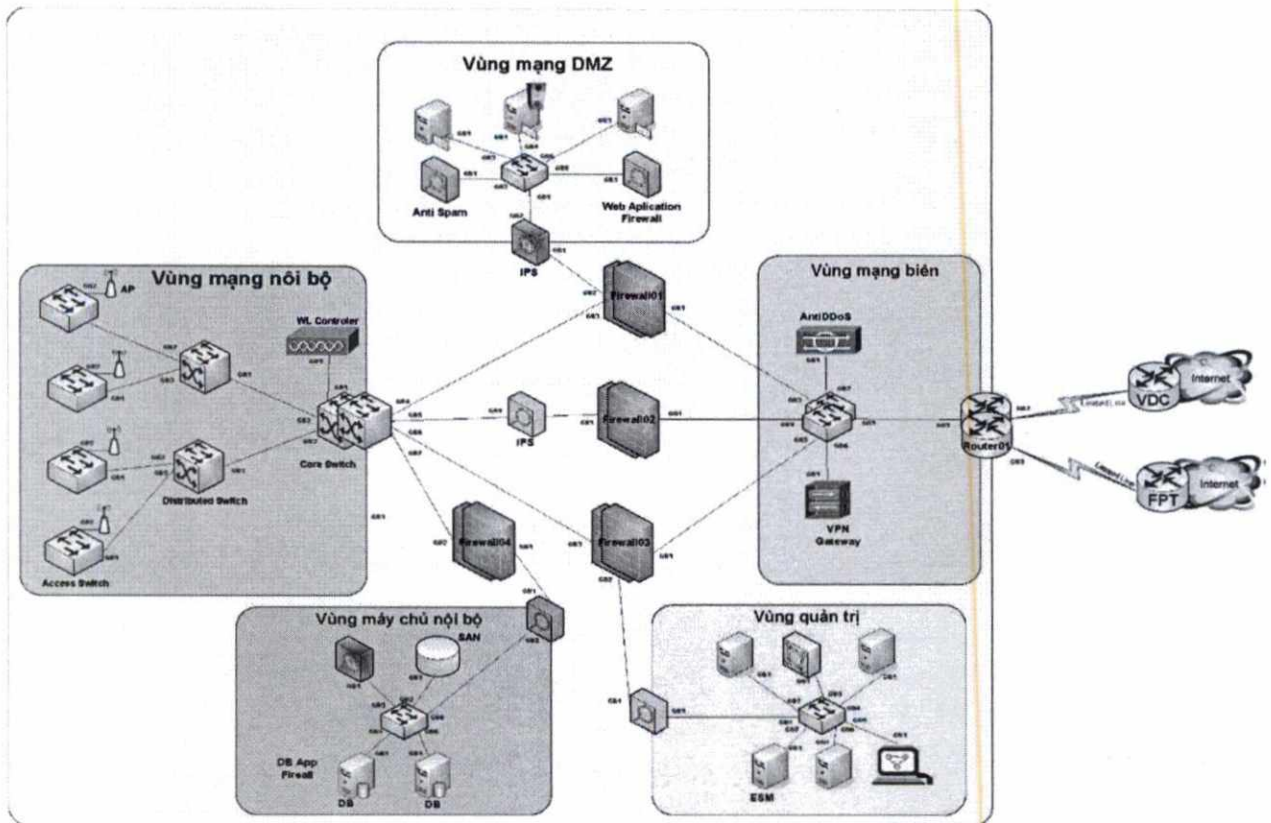
+ Vùng DMZ đặt các máy chủ công cộng, cung cấp dịch vụ ra bên ngoài Internet. Vùng mạng này triển khai thiết bị phòng chống xâm nhập IPS, thiết bị Web Application Firewall, thiết bị Anti-Spam (tích hợp trong Firewall).

+ 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



Kết nối vật lý của Hệ thống thông tin thị xã An Khê

c) Danh mục thiết bị sử dụng trong hệ thống

TT	Tên thiết bị/Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Router DrayTek Vigor 2912F, TotoLink F1	Vùng mạng biên	Kết nối và định tuyến động với các Router của 02 ISP
2	Firewall Sophos XG 135	Vùng DMZ	Quản lý truy cập và bảo vệ vùng mạng DMZ
3	Switch Cisco SF-200-24, TP-Link TL-SF-1008D; Complex PS22-16, Tenda S105.	Vùng mạng nội bộ	Chuyển mạch để kết nối các thiết bị sử dụng mạng lại với nhau

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

TT	Tên dịch vụ	Máy chủ triển khai	Mục đích sử dụng
1	Dự phòng các Hệ thống dùng chung cấp xã	Máy chủ IBM System X3200 M3/ Vùng máy chủ nội bộ/ Windows Server 2008 Standard SP1	Dự phòng và lưu trữ dữ liệu các Hệ thống dùng chung cấp xã: Hệ thống Một cửa điện tử; Hệ thống quản lý văn bản và điều hành.
2	Dự phòng các Hệ thống dùng chung thị xã	Máy chủ IBM System X650 M4/ Vùng máy chủ nội bộ/ Windows Server 2008 Standard SP1	Dự phòng và lưu trữ dữ liệu các Hệ thống dùng chung thị xã: Hệ thống Một cửa điện tử; Hệ thống quản lý văn bản và điều hành.
3	Hệ thống Một cửa điện tử; Hệ thống quản lý văn bản và điều hành cấp xã.	Máy chủ Lenovo System X3650 M5/ Vùng máy chủ nội bộ/ Windows Server 2012 Standard SP1	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. 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.
4	Hệ thống Một cửa điện tử; Hệ thống quản lý văn bản và điều hành thị xã.	Máy chủ Lenovo System X3650 M5/ Vùng máy chủ nội bộ/ Windows Server 2012 Standard SP1	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. 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.

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

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

TT	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 chung của các cơ quan, đơn vị thuộc thị xã.	2	Khoản 3, Điều 8 Nghị định số 85/2016/NĐ-CP
2	Cổng/ Trang thông tin điện tử của thị xã/xã	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 8 Nghị định số 85/2016/NĐ-CP
3	Hệ thống mạng nội bộ - LAN của các cơ quan trong thị xã		Hệ thống cơ sở hạ tầng thông tin phục vụ hoạt động các cơ quan, đơn vị thuộc thị xã.	2	Khoản 3, Điều 8 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

- Việc bảo đảm an toàn thông tin mạng là yêu cầu bắt buộc trong quá trình thiết kế, xây dựng, vận hành, nâng cấp, sử dụng và hủy bỏ trong ứng dụng CNTT của các cơ quan, đơn vị trên địa bàn thị xã.

- Việc thực hiện các phương pháp bảo đảm 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; 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; Quyết định số 41/2016/QĐ-UBND ngày 30/9/2016 của UBND tỉnh Gia Lai về ban hành quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của cơ quan nhà nước trên địa bàn tỉnh Gia Lai; Quyết định số 3618/QĐ-UBND ngày 13/12/2017 của Ủy ban nhân dân thị xã An Khê về việc ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn thị xã An Khê và các quy định của pháp luật có liên quan.

- Thủ trưởng các cơ quan, đơn vị là người chịu trách nhiệm trực tiếp chỉ đạo công tác bảo đảm an toàn thông tin mạng tại đơn vị mình.

- Bố trí nguồn lực phù hợp với quy mô, điều kiện của cơ quan nhằm thực hiện tốt nhất công tác bảo đảm an toàn thông tin mạng.

- Những văn bản có chứa nội dung bí mật nhà nước phải được quản lý theo chế độ mật theo quy định của pháp luật hiện hành. Không được truyền tải trên mạng và phải được mã hóa theo quy định của Luật Cơ yếu ngày 26/11/2011.

- Hoạt động bảo đảm an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, hiệu quả trên cơ sở tuân thủ tiêu chuẩn, quy chuẩn, quy định về an toàn thông tin mạng.

1.2. Trách nhiệm trong an toàn thông tin

- Trách nhiệm của Lãnh đạo cơ quan, đơn vị:

+ Tổ chức chỉ đạo thực hiện các quy định tại Quy chế này và chịu trách nhiệm trong công tác bảo đảm an toàn thông tin mạng của cơ quan, đơn vị.

+ Tạo điều kiện để cán bộ, công chức được học tập, nâng cao trình độ về an toàn thông tin mạng.

+ Bố trí, tạo điều kiện cho công chức, viên chức chuyên trách về công nghệ thông tin được ưu tiên bồi dưỡng nghiệp vụ về an toàn thông tin mạng.

+ Phối hợp, cung cấp thông tin và tạo điều kiện cho các đơn vị có thẩm quyền triển khai công tác kiểm tra khắc phục sự cố xảy ra một cách kịp thời, nhanh chóng và đạt hiệu quả.

+ Hằng năm, quan tâm bố trí kinh phí cho việc đào tạo an toàn thông tin, ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng nói riêng trong nội bộ cơ quan.

- Trách nhiệm của công chức, viên chức và người lao động được giao phụ trách an toàn thông tin mạng của đơn vị:

+ Chịu trách nhiệm bảo đảm an toàn thông tin mạng của đơn vị.

+ Tham mưu lãnh đạo cơ quan thực hiện các quy chế, quy trình nội bộ, triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng.

+ Thực hiện việc giám sát, đánh giá, báo cáo Lãnh đạo các rủi ro mất an toàn thông tin mạng và mức độ nghiêm trọng của các rủi ro đó.

+ Phối hợp với các cá nhân, đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng.

+ Thường xuyên cập nhật nâng cao kiến thức, trình độ chuyên môn đáp ứng yêu cầu bảo đảm an toàn thông tin mạng của đơn vị.

- Trách nhiệm của công chức, viên chức, người lao động trong các cơ quan, đơn vị:

+ 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.

+ Mỗi công chức, viên chức và người lao động phải 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 Văn phòng, hoặc Phòng Văn hóa và Thông tin để kịp thời ngăn chặn và xử lý.

+ Tham gia các chương trình đào tạo, hội nghị về an toàn thông tin mạng.

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, sử dụng các thiết bị CNTT, soạn thảo và lưu trữ văn bản mật của cơ quan, đơn vị thuộc thị xã.

1.4. Tổ chức bảo đảm an toàn thông tin

- Bảo đảm an toàn thông tin mức vật lý: Bảo vệ hệ thống hạ tầng kỹ thuật, phần mềm, ứng dụng và cơ sở dữ liệu khỏi các mối nguy hiểm vật lý (như: cháy, nổ; nhiệt độ, độ ẩm ngoài mức cho phép; thiên tai; mất điện; tác động cơ học) có thể gây ảnh hưởng đến hoạt động hệ thống.

- Bảo đảm an toàn thông tin khi sử dụng máy tính: Các cá nhân sử dụng máy tính để xử lý công việc tuân thủ: Chỉ cài đặt phần mềm hợp lệ (phần mềm có bản quyền hoặc phần mềm mã nguồn mở có nguồn gốc rõ ràng) và được phép sử dụng, chỉ truy nhập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông

tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy nhập thông tin cá nhân.

- Bảo đảm an toàn thông tin đối với mạng máy tính (mạng Lan, Internet) tại đơn vị.

- Bảo đảm an toàn thông tin mức dữ liệu: Bảo đảm tính bí mật, nguyên vẹn và khả dụng của thông tin, dữ liệu; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản.

- Bảo đảm an toàn thông tin khi tiếp nhận, phát triển, vận hành và bảo trì hệ thống thông tin: Khi tiếp nhận, phát triển, nâng cấp, bảo trì hệ thống thông tin, cơ quan, đơn vị phải tiến hành phân tích, xác định các rủi ro có thể xảy ra, đánh giá phạm vi tác động và phải chuẩn bị các biện pháp hạn chế, loại trừ các rủi ro này và yêu cầu các bên cung cấp, thi công, các cá nhân liên quan thực hiện.

1.5. Bảo đảm nguồn nhân lực

- Đảm bảo nhân sự chuyên trách về CNTT là công chức Văn phòng HĐND và UBND thị xã, Phòng Văn hóa và Thông tin thị xã, có trình độ CNTT từ Đại học trở.

- Có kế hoạch và định kỳ hàng năm, tổ chức đào tạo, bồi dưỡng, tuyên truyền, phổ biến nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ, công chức; cử công chức chuyên trách CNTT tham gia lớp tập huấn bồi dưỡng nâng cao của Sở Thông tin và Truyền thông tỉnh.

1.6. Quản lý thiết kế, xây dựng hệ thống (cấp độ 2 trở lên)

- 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

- Tùy theo tình hình thực tế triển khai ứng dụng CNTT, Phòng Văn hóa và Thông tin, Văn phòng HĐND và UBND thị xã thực hiện việc quản lý và kiểm soát để ngăn ngừa các hiểm họa và duy trì an toàn cho các hệ thống thông tin của cơ quan, phần

mềm ứng dụng và các hệ thống thông tin dùng chung của thị xã được giao quản lý, vận hành. Các nội dung có thể bao gồm:

- + Phòng máy chủ và các thiết bị mạng quan trọng như tường lửa (firewall), thiết bị định tuyến (router), hệ thống máy chủ,... phải được đặt trong phòng máy chủ và có các biện pháp bảo vệ, ngăn chặn xâm nhập trái phép vào phòng máy chủ.

- + Bảo đảm an toàn môi trường vật lý (nhiệt độ, độ ẩm, ánh sáng,...) cho phòng máy chủ, các hệ thống hỗ trợ (máy điều hòa nhiệt độ, nguồn cấp điện, hệ thống chống sét, dự phòng nguồn điện, cáp quang truyền dẫn...) được an toàn và hoạt động ổn định, sẵn sàng.

- + Phòng máy chủ của các cơ quan là khu vực hạn chế tiếp cận và được lắp đặt hệ thống camera giám sát. Chỉ những người có trách nhiệm theo quy định của thủ trưởng cơ quan mới được phép vào phòng máy chủ.

- + Hệ thống máy chủ phải được dán nhãn, có sơ đồ đầu nối, thể hiện cụ thể về địa chỉ IP, tên máy chủ. Sơ đồ đầu nối phải được cập nhật nếu có sự thay đổi.

- + Sử dụng thiết bị tường lửa, thiết bị phát hiện, ngăn chặn xâm nhập trái phép và các trang thiết bị khác nhằm bảo đảm an toàn bảo mật thông tin.

- + Thiết lập, cấu hình đầy đủ các tính năng của thiết bị an ninh mạng.

- + Sử dụng các công cụ để dò tìm và phát hiện kịp thời các điểm yếu, lỗ hổng và các truy cập bất hợp pháp vào hệ thống mạng và Hệ thống máy chủ của thị xã.

- + Thường xuyên kiểm tra, cập nhật các bản vá lỗi từ nhà sản xuất, phát hành.

- Ứng dụng chữ ký số chuyên dùng để bảo đảm an toàn thông tin mạng trong việc triển khai ứng dụng CNTT trong hoạt động của cơ quan và phục vụ công dân, tổ chức. Chữ ký số của cơ quan, đơn vị được Văn thư quản lý, bảo quản và sử dụng để ký các văn bản điện tử do cơ quan, đơn vị phát hành. Chữ ký số của cá nhân lãnh đạo cơ quan, đơn vị do lãnh đạo trực tiếp quản lý và sử dụng.

- Các cơ quan, đơn vị khai thác, sử dụng các ứng dụng, hệ thống thông tin theo đúng chức năng, nhiệm vụ được giao, bảo đảm phục vụ tốt công tác chuyên môn, nghiệp vụ của cơ quan.

- Trong quá trình vận hành hệ thống các cơ quan, đơn vị cần thực hiện quy định về phòng chống virus, mã độc đáp ứng các yêu cầu cơ bản như: Kiểm tra, diệt virus và mã độc trên các phương tiện mang thông tin, dữ liệu nhận từ bên ngoài trước khi sử dụng; không mở các thư điện tử lạ, các tập tin đính kèm hoặc các liên kết trong các thư lạ để tránh virus, mã độc; không vào các trang thông tin điện tử hoặc mở các email không rõ nguồn gốc xuất xứ, đáng ngờ; không tải các trò chơi vào máy hoạt động công vụ; không tự ý cài đặt các phần mềm không rõ nguồn gốc, không có bản quyền;

trong trường hợp phát hiện nhưng không diệt được virus, mã độc thì cần báo ngay cho người quản trị hệ thống xử lý.

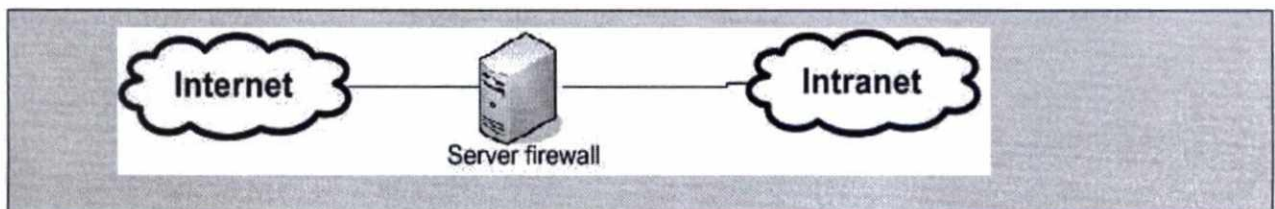
1.8. Kiểm tra, đánh giá và quản lý rủi ro: Thực hiện kiểm tra bảo mật hằng ngày, định kỳ mỗi tuần một lần; thực hiện sao lưu dữ liệu hằng ngày, sao lưu toàn bộ hệ thống vào ngày thứ 7 và chủ nhật.

2. Yêu cầu kỹ thuật

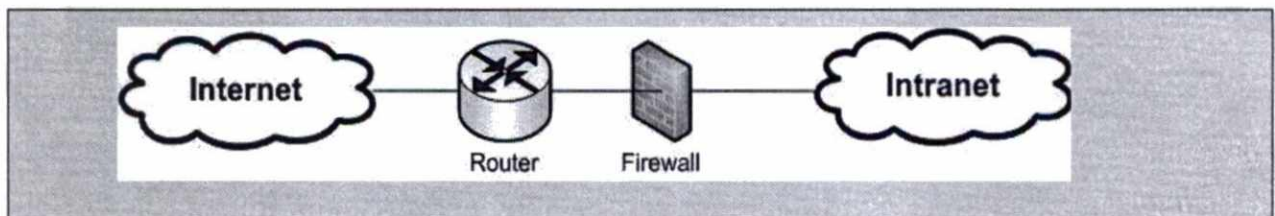
2.1. Bảo đảm an toàn mạng (cấp độ 2 trở lên)

a) Thiết kế hệ thống:

- Phần mềm Firewall (tường lửa): Là những Firewall dưới dạng phần mềm được cài đặt trên Server, có tính linh hoạt cao: Có thể thêm, bớt các quy tắc, các chức năng: Hệ điều hành Windows Kaspersky Endpoint Security, Sophos XG 135.



- Firewall cứng: Là những firewall được tích hợp vào thiết bị phần cứng: Sophos XG 135, Router.



b) Kiểm soát truy cập từ bên ngoài mạng: Dùng Firewall thiết lập các Role, vùng DMZ cho phép bên ngoài truy cập vào hệ thống.

c) Kiểm soát truy cập từ bên trong mạng: Dùng Firewall thiết lập các Role, vùng DMZ cho phép ra ngoài internet, cài đặt phần mềm diệt Malware có bản quyền ở các máy Client.

d) Nhật ký hệ thống: Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống; Thường xuyên xem file log máy chủ, log Apache, log firewall.

e) Phòng chống xâm nhập: Thường xuyên kiểm tra, cập nhật phiên bản firmware các thiết bị mạng, các phần mềm diệt virus và các phần mềm tiện ích khác.

f) Phòng chống phần mềm độc hại trên môi trường mạng: Thiết lập Role, DMZ cho Router LAN để chống truy cập các trang web độc hại; chặn hoặc hạn chế cho truy cập ở một số cổng (Port).

g) Bảo vệ thiết bị hệ thống: Lắp đặt máy lạnh, hệ thống chống sét, ổn áp, tích điện để phòng, bảo vệ hệ thống.

2.2. Bảo đảm an toàn máy chủ

a) Xác thực: Cài đặt mật khẩu đăng nhập máy chủ với những ký tự đặc biệt, độ dài không dưới 08 ký tự, thay đổi mật khẩu tối thiểu 3 tháng/1 lần.

b) Kiểm soát truy cập: Kiểm soát quá trình truy cập từ bên ngoài bằng port, sử dụng VPN để truy cập từ xa.

c) Nhật ký hệ thống: Xem file log máy chủ, thông báo của các phần mềm security của hệ thống.

d) Phòng chống xâm nhập: Loại bỏ các tài khoản không sử dụng trên máy chủ; Sử dụng firewall của hệ điều hành và hệ thống để chặn hoặc hạn chế 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 phần mềm diệt virus có bản quyền dành cho máy chủ, máy client nội bộ.

f) Xử lý máy chủ khi chuyển giao: Sao lưu tất cả dữ liệu (nếu cần thiết) trước khi chuyển giao hoặc xóa sạch thông tin, dữ liệu trên máy chủ khi 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 từ 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 những ứng dụng có chữ ký số từ nhà cung cấp hoặc tác giả và 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 hằng ngày trong hệ thống.

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

c) Sao lưu dự phòng: Sao lưu dự phòng dữ liệu máy chủ, ứng dụng được thực hiện tự động Office với hệ thống NAS.
