

ỦY BAN NHÂN DÂN TỈNH ĐẮK LẮK
SỞ VĂN HÓA, THỂ THAO VÀ DU LỊCH

HỒ SƠ
HỒ SƠ ĐỀ XUẤT CẤP ĐỘ
CHO HỆ THỐNG THÔNG TIN
SỞ VĂN HÓA, THỂ THAO VÀ DU LỊCH

(kèm theo Công văn số ngày / /2022 của Sở Văn hóa, Thể thao và Du lịch)

MỤC LỤC

THUẬT NGỮ, TỪ VIẾT TẮT	2
DANH MỤC CÁC BẢNG	3
DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ	3
PHẦN I. THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN....	4
1. Thông tin Chủ quản hệ thống thông tin.....	4
2. Thông tin Đơn vị vận hành.....	4
3. Mô tả phạm vi, quy mô của hệ thống	4
4. Mô tả cấu trúc của hệ thống.....	5
4.1. Sơ đồ logic tổng thể	5
4.2. Sơ đồ kết nối vật lý	6
4.3. Danh mục thiết bị sử dụng trong hệ thống	6
4.4. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống.....	7
4.5. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống.....	7
PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT	8
1. Danh mục hệ thống thông tin và cấp độ đề xuất.....	8
2. Thuyết minh đề xuất cấp độ đối với hệ thống thông tin.....	8
PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN HỆ THỐNG THÔNG TIN VỀ QUẢN LÝ	8
1. Thiết lập chính sách an toàn thông tin	Error! Bookmark not defined.
2. Tổ chức bảo đảm an toàn thông tin...	Error! Bookmark not defined.
3. Bảo đảm nguồn nhân lực.....	Error! Bookmark not defined.
4. Quản lý thiết kế, xây dựng hệ thống thông tin	Error! Bookmark not defined.
5. Quản lý vận hành hệ thống thông tin	Error! Bookmark not defined.
PHẦN IV. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ KỸ THUẬT	
1. Bảo đảm an toàn mạng	14
2. Bảo đảm an toàn máy chủ	Error! Bookmark not defined.
3. Bảo đảm an toàn ứng dụng	16

THUẬT NGỮ, TỪ VIẾT TẮT

ST T	Từ viết tắt	Nghĩa đầy đủ
1.	CNTT	Công nghệ thông tin
2.	CSDL	Cơ sở dữ liệu
3.	LAN	Mạng nội bộ
4.	WAN	Mạng tin học diện rộng
5.	VPN	Vitural Private Network
6.	DNS	Domain Name Server
7.	ATTT	An toàn thông tin
8.	TTĐT	Thông tin điện tử
9.	TDLCD	Truyền số liệu chuyên dùng

DANH MỤC CÁC BẢNG

Bảng 1. Danh mục thiết bị sử dụng trong hệ thống	7
Bảng 2. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống	7
Bảng 3. Quy hoạch địa chỉ IP các vùng mạng trong hệ thống.....	7

DANH MỤC CÁC HÌNH VẼ, ĐỒ THỊ

Hình 1. Cấu trúc logic của hệ thống	5
Hình 2. Kết nối vật lý của hệ thống	6

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

1. Thông tin Chủ quản hệ thống thông tin

- **Tên Tổ chức: Sở Văn hóa, Thể thao và Du lịch**
- Quy định chức năng, nhiệm vụ và quyền hạn:
- Người đại diện: Ông Thái Hồng Hà, Chức vụ: Giám đốc
- Địa chỉ: Địa chỉ trụ sở của đơn vị: Số 48 Nguyễn Tất Thành, thành phố Buôn Ma Thuột, tỉnh Đắk Lắk.
- Thông tin liên hệ: Số điện thoại: 0262 3852 409

2. Thông tin Đơn vị vận hành

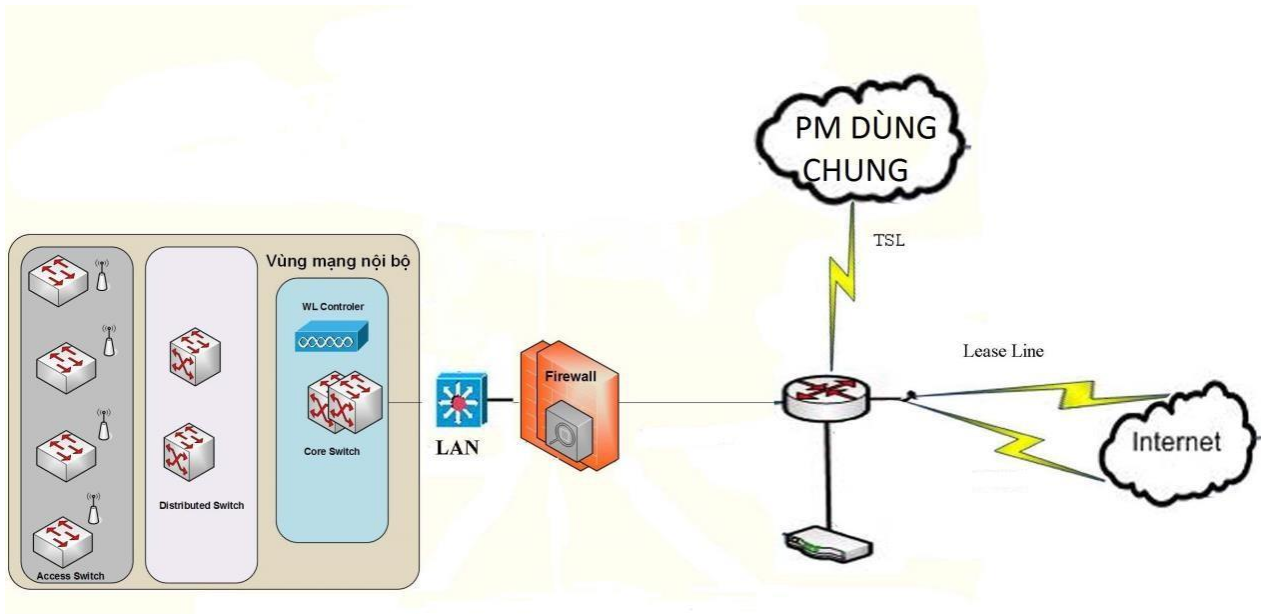
- **Tên Đơn vị vận hành: Hệ thống mạng LAN phục vụ công tác chỉ đạo, điều hành, hoạt động nội bộ cơ quan Sở Văn hóa, Thể thao và Du lịch**
- Quy định chức năng, nhiệm vụ và quyền hạn: Quyết định số 588/QĐ-SVHTTDL ngày 16/9/2020.
- Người đại diện: Ông Thái Hồng Hà, Chức vụ: Giám đốc
- Địa chỉ: Địa chỉ trụ sở của đơn vị: Số 48 Nguyễn Tất Thành, thành phố Buôn Ma Thuột, tỉnh Đắk Lắk.

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống thông tin Sở Văn hóa, Thể thao và Du lịch: Hệ thống mạng LAN phục vụ công tác chỉ đạo điều hành, hoạt động nội bộ cơ quan Sở Văn hóa, Thể thao và Du lịch.
- Đối tượng phục vụ của Hệ thống thông tin Sở Văn hóa, Thể thao và Du lịch: Các Phòng chuyên môn, đơn vị sự nghiệp thuộc Sở; Người dân, doanh nghiệp.
- Danh mục các hệ thống thông tin thành phần/các dịch vụ được cung cấp bởi Hệ thống thông tin Sở Văn hóa, Thể thao và Du lịch:
 - + Hệ thống mạng nội bộ (LAN)
 - + Hệ thống Trang/Cổng thông tin điện tử: <http://vhttdl.daklak.gov.vn>.
 - + Hệ thống Phòng họp trực tuyến

4. Mô tả cấu trúc của hệ thống

4.1. Sơ đồ logic tổng thể

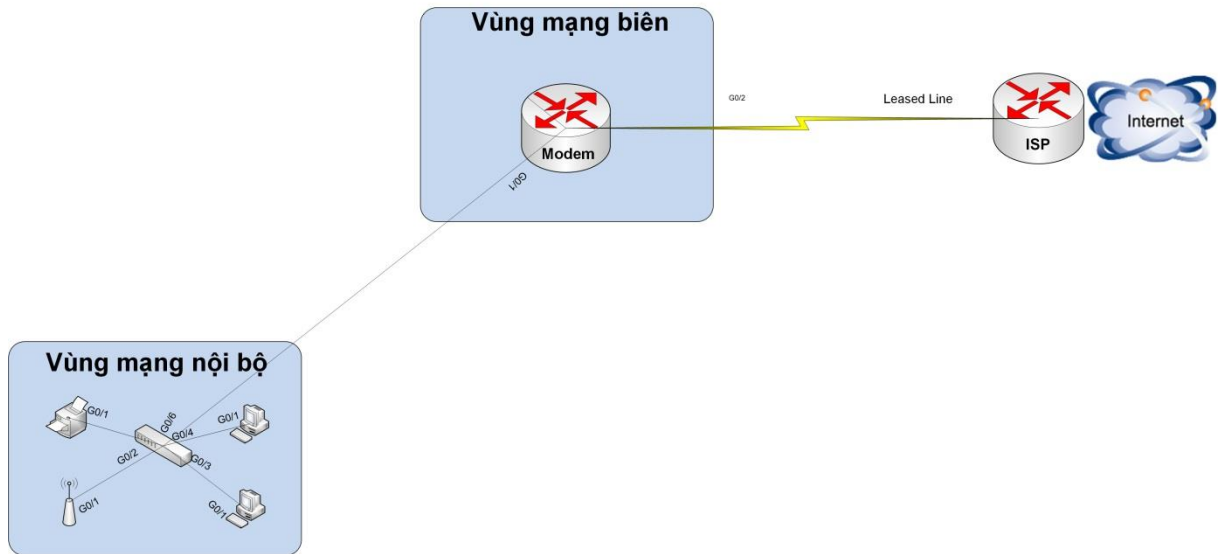


Hình 1. Cấu trúc logic của hệ thống

Các vùng mạng được thiết kế như sau:

- + Vùng mạng biên được thiết kế để kết nối hệ thống ra các mạng bên ngoài và mạng Internet.
- + Vùng mạng nội bộ đặt các thiết bị nội bộ, cung cấp các dịch vụ nội bộ cho người sử dụng trong hệ thống.

4.2. Sơ đồ kết nối vật lý



Hình 2. Kết nối vật lý của hệ thống

- Vùng Internet là nơi cung cấp dịch vụ Internet cho toàn bộ hệ thống. Các chức năng chính của vùng Internet gồm:
 - + Cung cấp đường truyền truy cập Internet cho tất cả các người dùng.
 - + Cung cấp cơ sở hạ tầng Internet để triển khai các ứng dụng phần mềm dùng chung của Tỉnh.
 - + Đảm bảo an ninh, an toàn hệ thống khỏi các mối nguy hiểm từ bên ngoài Internet.

4.3. Danh mục thiết bị sử dụng trong hệ thống

STT	Tên thiết bị/ Chủng loại	Vị trí triển khai	Mục đích sử dụng

1	Modem/VNPT	Vùng mạng biên	Kết nối và định tuyến động với các Router của ISP.
02	Switch/Cisco SG92	DC User	Access Switch cho người dùng
03	PC	DC User	Các máy trạm cho người dùng

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

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

STT	Tên dịch vụ	Máy chủ/Ứng dụng cài đặt/Vùng mạng/HĐH	Mục đích sử dụng
1	Trang/Cổng thông tin điện tử	Server01/Cài đặt Web-App	Cung cấp thông tin công khai cho người sử dụng.
2	DHCP	Modem, Router/VNPT	Cấp phát ip động
3	FireWall	Modem, Router/VNPT	Kiểm soát các truy cập mạng

Bảng 2. Danh mục các ứng dụng/dịch vụ cung cấp bởi hệ thống

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

- Quy hoạch địa chỉ IP tính theo từng phòng, ban chuyên môn để hạn chế trùng địa chỉ IP.

- Quy hoạch địa chỉ IP cho hệ thống Wifi riêng để không ảnh hưởng đến dãy IP trong hệ thống.

STT	Vùng mạng	IP Private	IP Public
01	Vùng mạng nội bộ	192.168.11.1/24	103.35.64.173
02	Vùng mạng nội bộ	192.168.1.1/24	103.35.64.173

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

PHẦN II. THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

Hệ thống thông tin của Sở Văn hóa, Thể thao và Du lịch bao gồm hệ thống thành phần với cấp độ đề xuất tương ứng, bao gồm:

ST T	Hệ thống	Cấp độ đề xuất	Căn cứ đề xuất
1	Hệ thống mạng nội bộ (LAN)	2	khoản 3 Điều 8 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và tại điểm a khoản 5 Điều 4 Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông

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

Hệ thống mạng nội bộ Sở Văn hóa, Thể thao và Du lịch là tập hợp trang thiết bị, đường truyền dẫn kết nối phục vụ chung hoạt động của các phòng chuyên môn thuộc Sở Văn hóa, Thể thao và Du lịch. Căn cứ theo quy định tại khoản 3 Điều 8 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và tại điểm a khoản 5 Điều 4 Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông, hệ thống này được đề xuất cấp độ 2.

PHẦN III. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ QUẢN LÝ

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

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

- Bảo vệ thông tin, hệ thống thông tin nội bộ, hạn chế việc bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

- Hoạt động an toàn thông tin mạng tại Sở Văn hóa, Thể thao và Du lịch phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật

nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

- Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

- Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

- Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

- Việc đầu tư trang thiết bị phần cứng, phần mềm và các giải pháp bảo vệ phải được thực hiện đồng bộ, tránh đầu tư trùng lặp.

- Bố trí nguồn kinh phí để bảo đảm an toàn hệ thống thông tin thực hiện theo thứ tự ưu tiên từ cấp độ cao xuống cấp độ thấp.

2. Trách nhiệm bảo đảm an toàn thông tin

Quy định trách nhiệm của phòng, ban chuyên môn, các đơn vị sự nghiệp trực thuộc sử dụng chung hệ thống mạng LAN tại Sở Văn hóa, Thể thao và Du lịch; sử dụng, vận hành khai thác phòng họp trực tuyến; đăng tải thông tin trên Cổng Thông tin điện tử Bim Sơn trong việc bảo đảm an toàn thông tin.

- Sở Văn hóa, Thể thao và Du lịch có trách nhiệm thực hiện các nhiệm vụ quản lý hệ thống thông tin theo quy định tại Điều 20, Nghị định 85/2016/NĐ-CP.

- Văn phòng Sở:

- + Tham mưu Ban Giám đốc Sở tổ chức thực thi, đôn đốc, giám sát công tác đảm bảo an toàn thông tin trong hệ thống thông tin nội bộ tại cơ quan theo quy định tại Điều 21, Nghị định 85/2016/NĐ-CP.

- + Đảm bảo vận hành tốt đối với hệ thống thông tin thuộc phạm vi quản lý.

- + Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nội bộ cơ quan.

- + Chủ trì, phối hợp với các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng định kỳ hàng năm hoặc theo chỉ đạo của Ban Giám đốc Sở.

- + Tùy theo mức độ sự cố, phối hợp với Sở Thông tin & Truyền thông và các đơn vị có liên quan xử lý, ứng cứu các sự cố an toàn thông tin mạng.

- + Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ của Sở Thông tin và Truyền thông.

+ Hàng năm cử cán bộ chuyên trách quản trị mạng tham gia các chương trình đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng do các sở, ban ngành cấp tỉnh tổ chức.

+ Tổ chức tuyên truyền, hướng dẫn về công tác bảo đảm an toàn thông tin mạng trên các phương tiện thông tin đại chúng và trên Cổng TTĐT Sở.

+ Hàng năm lập dự toán kinh phí cho việc 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 ; lập kế hoạch nâng cấp, bảo trì, sửa chữa, cài đặt phần mềm diệt virus bản quyền... Đề xuất sửa chữa, nâng cấp, thay thế trang thiết bị không phù hợp để đảm bảo an toàn thông tin trong toàn hệ thống.

- Trách nhiệm của các phòng, ban chuyên môn thuộc Sở:

+ Trưởng các phòng, ban chuyên môn chỉ đạo công chức của phòng mình thực hiện nghiêm các quy định bảo đảm an toàn thông tin trong toàn hệ thống mạng LAN cơ quan, không sử dụng các thiết bị ngoại vi để sao chép, chia sẻ thông tin, dữ liệu.

+ Nâng cao ý thức trách nhiệm của cán bộ, công chức thuộc phòng, ban quản lý về đảm bảo an toàn thông tin trong hệ thống mạng LAN cơ quan.

+ Phối hợp với Văn phòng Sở trong công tác kiểm tra, phát hiện, xử lý kịp thời các sự cố về an toàn thông tin mạng.

- Trách nhiệm của cán bộ, công chức, viên chức, người lao động trong cơ quan.

+ 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.

+ Tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; Khai thác, sử dụng có hiệu quả các phần mềm dùng chung của tỉnh.

+ Không sử dụng USB để chia sẻ dữ liệu.

+ Tìm kiếm thông tin trên mạng từ các trang chính thống và tìm kiếm văn bản trên Trang Luật Việt Nam đã hợp đồng mua bản quyền truy cập hàng năm) và Trang quy phạm pháp luật của Tỉnh.

+ Phối hợp với quản trị mạng cơ quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng.

3. Phạm vi chính sách an toàn thông tin

- Đảm bảo an toàn thông tin trong toàn hệ thống mạng LAN cơ quan; Công TTĐT Sở; thực hiện gửi nhận, xử lý văn bản điện tử đảm bảo an toàn, bí mật Nhà nước.

- Chính sách bảo đảm an toàn thông tin trong hoạt động nội bộ cơ quan phải có các quy định và ràng buộc cụ thể mà mỗi cán bộ, công chức, viên chức, người lao động trong cơ quan phải tuân thủ khi tham gia vào hệ thống khai thác tài nguyên thông tin; phù hợp tình hình thực tế tại Sở Văn hóa, Thể thao và Du lịch.

4. Tổ chức bảo đảm an toàn thông tin

Mục tiêu là đưa ra mô hình, cách thức tổ chức cho các phòng, ban, cá nhân liên quan để đảm bảo việc xây dựng, triển khai và thực hiện tuân thủ các chính sách về an toàn thông tin được xây dựng, triển khai tại Sở Văn hóa, Thể thao và Du lịch; Duy trì đảm bảo an toàn thông tin trong hoạt động nội bộ; cung cấp thông tin phục vụ người dân, tổ chức, doanh nghiệp ngày càng tốt hơn.

4.1. Đơn vị chủ trì

- Văn phòng Sở chủ trì phối hợp với các phòng, ban chuyên môn liên quan thực hiện tốt quy chế đảm bảo an toàn thông tin trong hệ thống mạng LAN.

- Là đầu mối tổ chức thực hiện, tiếp nhận và xử lý các sự cố cơ bản về an toàn thông tin trong hoạt động nội bộ cơ quan.

- Phối hợp với Sở Thông tin & Truyền thông Thanh Hóa và các đơn vị liên quan kịp thời xử lý những sự cố mất an toàn thông tin ngoài khả năng xử lý của phòng.

4.2. Người sử dụng

- Người sử dụng có trách nhiệm quản lý tài khoản đối với các phần mềm dùng chung; thực hiện nghiêm các quy định về đảm bảo an toàn thông tin trong hệ thống mạng LAN cơ quan.

- Tự quản lý, bảo quản thiết bị mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

4.3. Cán bộ quản lý và vận hành hệ thống

- Xây dựng quy chế đảm bảo an toàn thông tin trong toàn hệ thống.

- Theo dõi cán bộ, CC, VC nghỉ hưu, thay đổi vị trí công tác để hủy bỏ, thay đổi tài khoản đăng nhập các phần mềm cho phù hợp.

- Tham gia các chương trình đào tạo về an toàn thông tin do các sở, ban, ngành cấp tỉnh tổ chức.

4.4. Quản lý sự cố an toàn thông tin

Cán bộ Quản trị mạng cơ quan có trách nhiệm:

- Phối hợp với Sở Thông tin & Truyền thông và các sở, ban, ngành liên quan phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/NĐ-CP của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; 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 xây dựng quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13,14 Quyết định số 05/2017/NĐ-CP .

- Phối hợp triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16 Quyết định số 05/2017/NĐ-CP .

- Phối hợp với các sở, ban, ngành cấp tỉnh hỗ trợ trong việc xử lý, khắc phục sự cố an toàn thông tin.

4.5. Quản lý an toàn người sử dụng

Thông tin, báo cáo kịp thời cho cán bộ Quản trị mạng 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.

5. Bảo đảm nguồn nhân lực

Mỗi cán bộ, công chức, viên chức trong Sở Văn hóa, Thể thao và Du lịch phải nắm rõ vai trò, trách nhiệm của mình khi tham gia vận hành, khai thức, xử lý thông tin trên môi trường mạng trong hệ thống .mạng LAN cơ quan; Nhằm giảm thiểu các rủi ro về việc lộ lọt thông tin, bí mật nhà nước; rà soát, tổng hợp danh sách các cá nhân đã nghỉ hưu hoặc chuyển công tác để loại ra khỏi hệ thống.

6. Quản lý vận hành hệ thống

6.1. Đối với thiết bị CNTT

- Phải lắp đặt thiết bị chống sét để bảo vệ hệ thống CNTT trong mạng LAN.
- Thiết bị chuyển mạch (switch) trong 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 và không 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 hệ thống mạng LAN, hỗ trợ chức năng xác thực thiết bị và người sử dụng...

- Phải có thiết bị Tường lửa (firewall) nhằm hạn chế việc truy cập trái phép từ bên ngoài.

6.2. Đối với Cổng TTĐT Sở Văn hóa, Thể thao và Du lịch

** Yêu cầu Viễn thông Đắc Lắc:*

- Là đơn vị mà Sở đã thuê dịch vụ hosting đặt Cổng TTĐT Sở Văn hóa, Thể thao và Du lịch thực hiện quản lý toàn bộ các phiên bản của mã nguồn, tổ chức mô hình trang web hợp lý, tránh nguy cơ tấn công; Phải cài đặt các hệ thống phòng vệ như tường lửa, thiết bị phát hiện/phòng chống xâm nhập (IDS/IPS) ở mức ứng dụng web.

- Các trang TTĐT thành phần khi đưa vào sử dụng hoặc khi bổ sung thêm các chức năng, dịch vụ công mới cần đánh giá kiểm định nhằm tránh được các lỗi bảo mật thường xảy ra trên ứng dụng web.

- Hàng tháng Viễn thông Đắc Lắc thực hiện việc backup toàn bộ nội dung trang web, gồm mã nguồn, cơ sở dữ liệu... để bảo đảm khi có sự cố có thể khắc phục lại trong thời gian nhanh nhất.

** Đối với quản trị website:*

- Quản trị website Cổng Thông tin điện tử Sở Văn hóa, Thể thao và Du lịch thực hiện bảo mật tài khoản quản trị, thường xuyên đổi mật khẩu đủ mạnh (ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt); tạo tài khoản và phân công quyền đăng tải một số nội dung cho các thành viên được phân công.

- Ban biên tập Cổng Thông tin điện tử thực hiện phân công nhiệm vụ cụ thể cho từng thành viên, mỗi thành viên được giao nhiệm vụ phải chịu hoàn toàn trách nhiệm trước Trưởng Ban và trước Pháp luật về những nội dung được phân công phụ trách; thực hiện đăng tải đầy đủ các nội dung theo quy định tại Nghị định số 43/2011/NĐ-CP.

6.3. Đối với hệ thống quản lý văn bản

** Đối với quản trị hệ thống*

- Có nhiệm vụ phân quyền truy cập cho các thành viên; điều chỉnh vị trí công tác cho người sử dụng (khi có sự thay đổi); xóa khỏi hệ thống các tài khoản người dùng đã về hưu hoặc chuyển công tác; Thường xuyên thay đổi mật khẩu quản trị đủ mạnh để đảm bảo an toàn, bảo mật thông tin. Mật khẩu có ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt.

- Hướng dẫn quy trình xử lý nội bộ trên các phần mềm dùng chung của Tỉnh cho cán bộ, công chức, viên chức tại cơ quan .

- Xây dựng quy trình nội bộ xử lý công việc trên phần mềm Một cửa điện tử cho phù hợp với chức danh và tình hình thực tế tại Cơ quan.

- Tham mưu cho Ban Giám đốc Sở các văn bản chỉ đạo, điều hành thực hiện quản lý, tiếp nhận, xử lý, ký số văn bản điện tử đảm bảo an toàn, hiệu quả.

** Đối với người dùng:*

- Thường xuyên đổi mật khẩu đủ mạnh (ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt) đối với các phần mềm dùng chung của tỉnh.

- Thực hiện xử lý công việc trên môi trường mạng và ký số cá nhân, đảm bảo theo đúng quy định. Chịu trách nhiệm về nội dung và thể thức văn bản tham mưu.

PHẦN IV. THUYẾT MINH PHƯƠNG ÁN BẢO ĐẢM AN TOÀN THÔNG TIN VỀ KỸ THUẬT

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

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

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

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

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có	Hệ thống được bảo vệ bởi tường lửa của Router, giúp ngăn chặn các cuộc tấn công mạng bằng cách theo dõi nhiều trạng thái hơn trong mỗi phiên. Nó xác nhận lưu

			<p>lượng truy cập đi qua mỗi phiên phù hợp giao thức.</p> <p>Hiện tại các kết nối tới các thiết bị nội bộ được thực hiện theo phương thức có dây; các kết nối không dây được thực hiện trên thiết bị di động phục vụ truy cập Internet được bảo mật và mã hóa dữ liệu.</p> <p>Các thiết bị hệ thống/máy chủ được thiết lập cấu hình cho phép quản trị từ xa an toàn.</p>
2	Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Có	<p>Truy cập giữa các vùng mạng được quản lý và phòng chống xâm nhập sử dụng Modem/VNPT có tích hợp chức năng phòng chống xâm nhập.</p>

1.2. Kiểm soát truy cập từ bên ngoài mạng

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

1.3. Bảo vệ thiết bị hệ thống

Yêu cầu	Cấu hình chức năng xác thực trên các thiết bị hệ thống (nếu hỗ trợ) để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa;	Thiết lập cấu hình chỉ cho phép sử dụng các kết nối mạng an toàn (Nếu hỗ trợ) khi truy cập, quản trị thiết bị từ xa.
Thiết bị		
Modem/VNPT	+	+

2. Bảo đảm an toàn ứng dụng

2.1. Xác thực

Yêu cầu	Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng	Lưu trữ có mã hóa thông tin xác thực hệ thống	Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng
Ứng dụng			
Trang/ Cổng thông tin điện tử	+	+	+

2.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị ứng dụng từ xa	Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng
Ứng dụng		
Trang/ Cổng thông tin điện tử	+	+

2.3. Nhật ký hệ thống

Yêu cầu	Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau: (1) Thông tin truy cập ứng dụng (2) Thông tin đăng nhập khi quản trị ứng dụng.
Ứng dụng	
Trang/ Cổng thông tin điện tử	+