ỦY BAN NHÂN DÂN TỈNH BẮC KẠN
BAN DÂN TỘC

HỒ SƠ
ĐỀ XUẤT CẤP ĐỘ HỆ THỐNG THÔNG TIN
BAN DÂN TỘC TỈNH BẮC KẠN

Bắc Kạn - 2022

ỦY BAN NHÂN DÂN TỈNH BẮC KẠN
BAN DÂN TỘC

THUYẾT MINH HỒ SƠ
ĐỀ XUẤT CẤP ĐỘ HỆ THỐNG THÔNG TIN CỦA BAN DÂN TỘC TỈNH BẮC KẠN

ĐƠN VỊ CHUYÊN TRÁCH VỀ AN TOÀN THÔNG TIN Sở Thông tin và Truyền thông	ĐƠN VỊ VẬN HÀNH HỆ THỐNG THÔNG TIN Ban Dân tộc
Phó Giám đốc	**Trưởng Ban**
Lô Quang Tuyến	**Triệu Thị Thu Phương**

Bắc Kạn - 2022

MỤC LỤC

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.	DVCTT	Dịch vụ công trực tuyến
4.	MCĐT	Một cửa điện tử
5.	WAN	Mạng diện rộng
6.	LAN	Mạng nội bộ
7.	TSLCD	Mạng Truyền số liệu chuyên dùng
8.	VPN	Vitural Private Network
9.	DNS	Domain Name Server

PHẦN I
THÔNG TIN TỔNG QUAN VỀ HỆ THỐNG THÔNG TIN

1. Chủ quản hệ thống thông tin: Ủy ban nhân dân tỉnh Bắc Kạn.

Tên tổ chức: Uỷ ban nhân dân tỉnh Bắc Kạn

Quy định chức năng, nhiệm vụ và quyền hạn: Luật Tổ chức Chính quyền địa phương số 77/2015/QH13 ngày 19/6/2015.

Người đại diện: Ông Nguyễn Đăng Bình, Chủ tịch UBND tỉnh Bắc Kạn

Địa chỉ: Tổ 1B, phường Phùng Chí Kiên, thành phố Bắc Kạn, tỉnh Bắc Kạn.

Thông tin liên hệ: Số điện thoại: 02093 870425 Fax: 02093 871751; Email: ubnd@backan.gov.vn

2. Đơn vị vận hành: Ban Dân tộc tỉnh Bắc Kạn

Ban Dân tộc được thành lập theo Quyết định số 1028/QĐ-UBND, ngày 18/5/2005 của Ủy ban nhân dân tỉnh, thực hiện chức năng tham mưu giúp Ủy ban nhân dân tỉnh quản lý nhà nước về công tác dân tộc trên địa bàn tỉnh.

Người đại diện: Triệu Thị Thu Phương, Trưởng Ban Dân tộc tỉnh Bắc Kạn.

Địa chỉ: Tổ 4, phường Đức Xuân, thành phố Bắc Kạn, tỉnh Bắc Kạn.

Thông tin liên hệ: 02093.812.456 Email: bandantoc@backan.gov.vn

3. Mô tả phạm vi, quy mô của hệ thống

- Phạm vi, quy mô của Hệ thống thông tin Ban Dân tộc: Hệ thống thông tin Ban Dân tộc được thiết lập để phục vụ công tác chỉ đạo điều hành, thực hiện các nhiệm vụ chuyên môn của Ban.

- Đối tượng phục vụ của hệ thống: Cán bộ, công chức thuộc Ban; các cơ quan, tổ chức, doanh nghiệp, cá nhân trên địa bàn tỉnh Bắc Kạn.

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

Hệ thống mạng nội bộ:

+ Hệ thống thông tin phục vụ hoạt động nội bộ;

+ Trang thông tin điện tử;

+ Hệ thống cơ sở hạ tầng thông tin nội bộ.

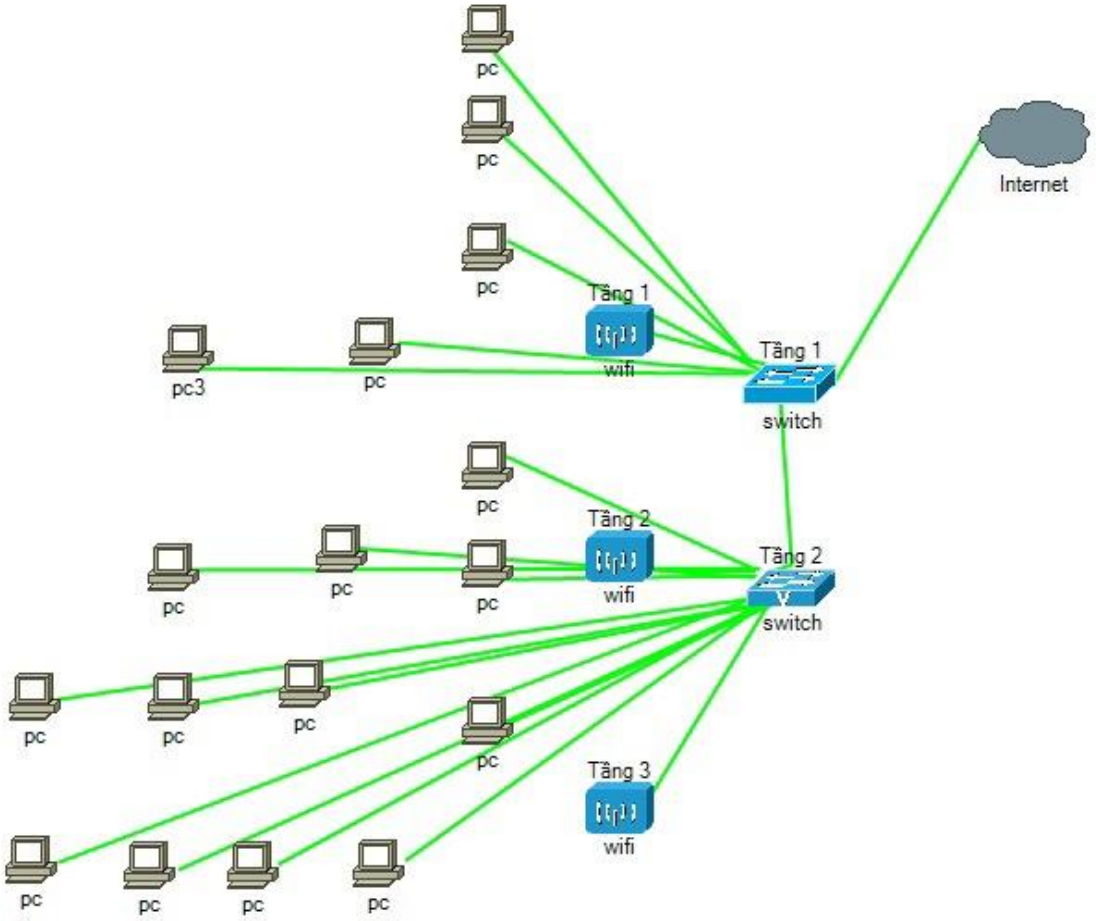
4. Mô tả cấu trúc của hệ thống

4.1. Cấu trúc vật lý

- Vùng mạng biên có nhiệm vụ kết nối hệ thống mạng của cơ quan ra các mạng bên ngoài và mạng Internet.

- Vùng mạng nội bộ được thiết lập để cung cấp kết nối mạng cho các máy trạm và thiết bị đầu cuối khác của người sử dụng vào hệ thống.

Sơ đồ kết nối vật lý



Hình 1: Sơ đồ kết nối vật lý của Hệ thống mạng

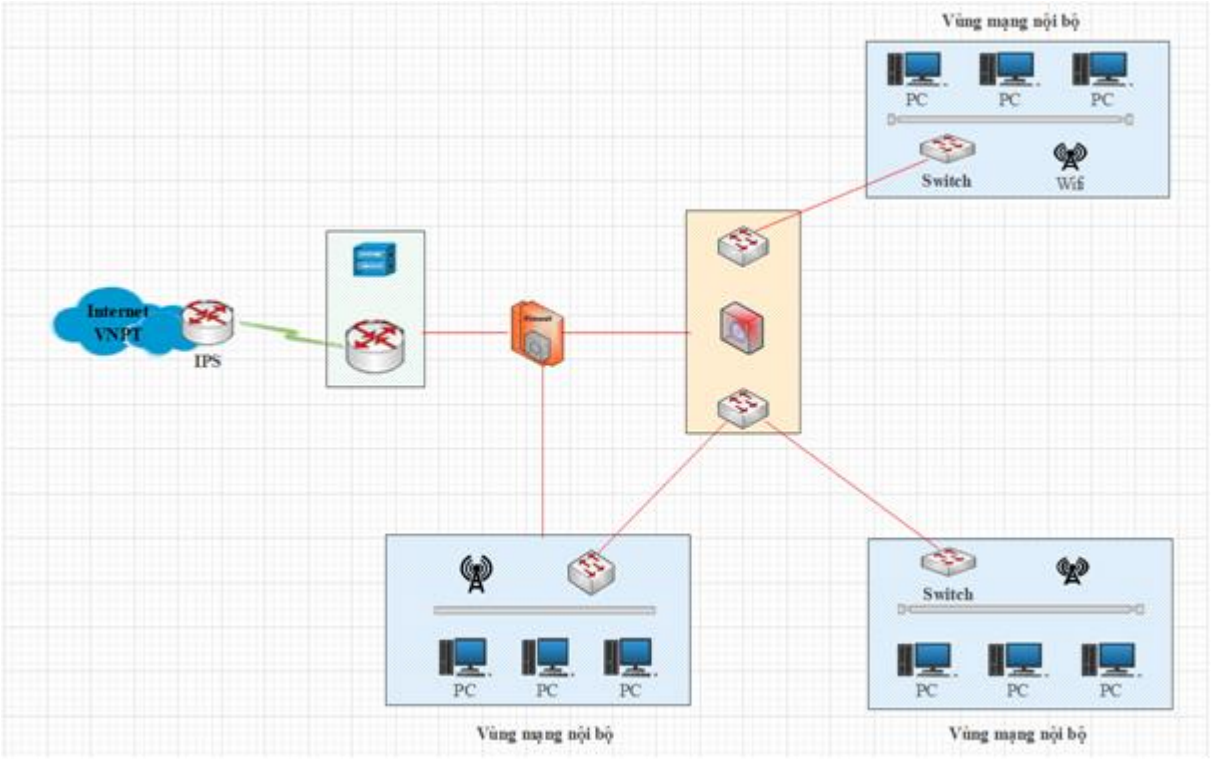
4.2. Cấu trúc logic

Các phân vùng mạng chính gồm:

- Vùng mạng biên: Được thiết kế để kết nối hệ thống mạng Ban Dân tộc cung cấp cổng kết nối VPN từ bên ngoài Internet vào và thiết bị kết nối phân vùng hệ thống ra các mạng bên ngoài và mạng Internet; vùng mạng này triển khai các thiết bị định tuyến, thiết bị cân bằng tải để bảo vệ toàn diện hệ thống mạng, phòng chống tấn công và các xâm nhập trái phép từ bên ngoài.

- Vùng mạng nội bộ: Đặt các thiết bị chuyển mạch để kết nối máy tính của người sử dụng trong cơ quan đơn vị với các hệ thống dữ liệu nội bộ, hệ thống mạng chuyên dụng để giải quyết công việc hàng ngày và kết nối ra ngoài mạng internet.

Sơ đồ logic tổng thể



Hình 2: Cấu trúc logic của hệ thống mạng Ban Dân tộc

4.3. Danh mục thiết bị sử dụng trong hệ thống

Trong hệ thống trang bị các thiết bị cơ bản như: thiết bị định tuyến Router (R), thiết bị chuyển mạch Switch (SW), đường truyền mạng và các thiết bị khác.

STT	Tên thiết bị/Chủng loại	Vị trí triển khai	Mục đích sử dụng
1	Router: Draytek Vigor 2912F - Đường truyền FTTH VNPT dung lượng 60Mps	Vùng mạng biên, là lớp ngoài cùng ra internet và từ internet kết nối vào	Thực hiện kết nối mạng Internet và sử dụng tường lửa (firewall) để quản lý truy cập vào/ra và bảo vệ hệ thống do nhà mạng VNPT cung cấp.
2	Mạng nội bộ: Hệ thống mạng nội bộ LAN, wifi JPLINK W750R, Switch TP-Link kết nối và các máy tính làm việc trong cơ quan.	Vùng mạng nội bộ	Sử dụng việc chuyển mạch; Quản lý truy cập vào/ra lớp mạng Lan cho người dùng

4.4. 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	Hệ thống Mạng nội bộ	Máy trạm/Ứng dụng cài đặt BKAV/Vùng mạng nội bộ/HĐH Windows	- Kết nối mạng cơ sở dữ liệu chuyên dùng. - Đảm bảo an toàn thông tin mạng.

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

STT	Vùng mạng	IP Private	IP Public
1	Vùng mạng nội bộ	10.80.42.1	14.228.133.124

PHẦN II
THUYẾT MINH CẤP ĐỘ ĐỀ XUẤT

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

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

TT	Hệ thống	Loại thông tin xử lý	Loại hình HTTT	Cấp độ đề xuất	Căn cứ đề xuất
1	Trang thông tin điện tử	Thông tin riêng của tổ chức, hỗ trợ cho việc thực hiện nhiệm vụ của ngành, cung cấp thông tin cho cá nhân, tổ chức.	Hệ thống thông tin phục vụ hoạt động ngành, người dân, doanh nghiệp	2	Khoản 1, khoản 2/Điều 8/NĐ85/2016
2	Hệ thống mạng nội bộ	Thông tin riêng/thông tin cá nhân	Hệ thống thông tin phục vụ hoạt động nội bộ	2	Khoản 3/Điều 8/NĐ85/2016

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

2.1. Trang Thông tin điện tử

Trang thông tin điện tử Ban Dân tộc là kênh thông tin chính thức của Ban Dân tộc trên địa bàn tỉnh trên mạng Internet để tuyên truyền đến người dân và doanh nghiệp trên địa bản tỉnh đường lối, chủ trương. chính sách của Đảng, pháp luật của Nhà nước về công tác dân tộc; tuyên truyền về công tác dân tộc, chính

sách dân tộc, các hoạt động trên lĩnh vực công tác dân tộc; các gương điển hình tiên tiến, các thành tích nổi bật trên lĩnh vực công tác dân tộc...

Căn cứ theo quy định tại Khoản 1 và điểm a, khoản 2/Điều 8/NĐ85/2016, hệ thống này được đề xuất bảo đảm an toàn hệ thống thông tin cấp độ 2.

2.2. Hệ thống mạng nội bộ

Phục vụ hoạt động nội bộ, quản trị, vận hành của đơn vị. Hệ thống cung cấp ứng dụng nội bộ cơ quan và lưu trữ số liệu nội bộ Ban Dân tộc tỉnh Bắc Kạn.

Căn cứ theo quy định tại Khoản 3/Điều 8/NĐ85/2016, hệ thống này được đề xuất bảo đảm an toàn hệ thống thông tin cấp độ 2

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

I. Thuyết minh phương án bảo đảm an toàn thông tin đáp ứng các yêu cầu an toàn cơ bản về Quản lý

1. Thiết lập chính sách an toàn thông tin

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

Việc bảo đảm an toàn trong toàn hệ thống thông tin phục vụ hoạt động của cơ quan Ban Dân tộc được đề xuất thực hiện theo cấp độ cao nhất trong hệ thống là cấp độ 2 đảm bảo duy trì thường xuyên, liên tục từ khâu thiết kế, xây dựng, vận hành đến khi hủy bỏ, luôn tuân thủ đầy đủ theo tiêu chuẩn, quy chuẩn kỹ thuật nhằm bảo vệ thông tin, hệ thống thông tin trên mạng tránh 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.

1.2. Nguyên tắc bảo đảm an toàn thông tin

Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân 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.

1.3. Xác định trách nhiệm đơn vị chuyên trách về an toàn thông tin và các đối tượng thuộc phạm vi điều chỉnh của chính sách an toàn thông tin

a) Ban Dân tộc là đơn vị vận hành chủ quản đối với hệ thống thông tin của Ban Dân tộc, do 01 đồng chí Phó Trưởng Ban trực tiếp chỉ đạo và phụ trách công tác bảo đảm an toàn thông tin trong hoạt động của cơ quan Ban Dân tộc theo quy định tại Điều 20, Nghị định 85.

b) Thanh tra và Văn phòng là đơn vị chủ trì, thực hiện trách nhiệm của đơn vị vận hành đối với hệ thống thông tin (*mạng nội bộ*) của Ban Dân tộc.

- Tham mưu lãnh đạo Ban ban hành các quy chế, quy trình về bảo đảm an toàn thông tin mạng và triển khai các giải pháp kỹ thuật bảo đảm an toàn thông tin mạng;

- 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 hệ thống của Ban.

- Phối hợp chặt chẽ với Sở Thông tin và Truyền thông, Công an tỉnh và các đơn vị liên quan khác trong công tác phòng ngừa, đấu tranh, ngăn chặn các hoạt động xâm phạm an toàn thông tin mạng. Định kỳ hằng năm hoặc theo chỉ đạo của tỉnh kiểm tra công tác bảo đảm an toàn thông tin mạng đối với hệ thống được giao quản lý.

- Khi có sự cố cần phối hợp với cơ quan chuyên trách về Công nghệ thông tin là Sở Thông tin và Truyền thông và các đơn vị có liên quan xử lý, ứng cứu các sự cố để đưa hệ thống thông tin hoạt động trở lại bình thường đảm bảo an toàn thông tin mạng của đơn vị.

- Hàng năm, cử cán bộ, công chức phụ trách công nghệ thông tin tham gia các chương trình đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng để nâng cao trình độ chuyên môn, cập nhật kiến thức, công nghệ mới đủ năng lực đảm đương nhiệm vụ bảo đảm an toàn hệ thống thông tin của đơn vị. Đồng thời thường xuyên tạo điều kiện để các cán bộ trong đơn vị được học tập, nâng cao trình độ về an toàn thông tin mạng.

- Hàng năm xây dựng kế hoạch để cấp có thẩm quyền duyệt, bố trí kinh phí cho việc ứng dụng công nghệ thông tin nói chung và công tác bảo đảm an toàn thông tin mạng.

- Thường xuyên tuyên truyền, hướng dẫn về công tác bảo đảm an toàn thông tin mạng, các biện pháp phòng tránh phá hoại hệ thống mạng cho cán bộ công chức, viên chức và người lao động trong cơ quan để chủ động phòng tránh tấn công phá hoại, đảm bảo an toàn thông tin trong đơn vị.

c) Trách nhiệm của các phòng chuyên môn, đơn vị thuộc Ban:

- Lãnh đạo các phòng chuyên môn, đơn vị thuộc Ban có trách nhiệm tổ chức

thực hiện các quy định về công tác bảo đảm an toàn thông tin mạng trong phòng, đơn vị mình phụ trách.

- Phân công công chức kiêm nhiệm phụ trách bảo đảm công tác công nghệ thông tin, an toàn thông tin mạng của đơn vị. Thường xuyên tạo điều kiện bồi dưỡng nghiệp vụ về an toàn thông tin mạng cho công chức được giao phụ trách công nghệ thông tin.

- 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.

d) Trách nhiệm của cán bộ, công chức và người lao động:

* Trách nhiệm của công chức kiêm nhiệm về an toàn thông tin:

- Thực hiện việc giám sát, đánh giá, báo cáo lãnh đạo cơ quan, đơn vị 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 người 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.

2. Tổ chức bảo đảm an toàn thông tin

Ban hành Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc.

2.1. Đơn vị bảo đảm về an toàn thông tin

Ban Dân tộc giao Thanh tra và Văn phòng là bộ phận chuyên trách về an toàn thông tin của cơ quan.

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

* Yêu cầu: Có quy định về việc phối hợp với những cơ quan tổ chức có thẩm quyền:

- Bộ phận Thanh tra và Văn phòng được phân công bảo an toàn thông có trách nhiệm phối hợp với Sở Thông tin & Truyền thông tin và các đơn vị có liên quan tiến hành kiểm tra công tác bảo đảm an toàn thông tin mạng.

* Phương án Phối hợp với những cơ quan tổ chức có thẩm quyền:

- Phối hợp với Sở Thông tin và Truyền thông tỉnh Bắc Kạn là đầu mối liên hệ, phối hợp quản lý về an toàn thông tin theo quy định tại Quyết định số 12/2017/QĐ-UBND ngày 18 tháng 5 năm 2017 của UBND tỉnh Ban hành Quy chế phối hợp phòng, chống các hành vi vi phạm pháp luật trong lĩnh vực thông tin và truyền thông trên địa bàn tỉnh Bắc, Kạn cụ thể:

- Phối hợp với Sở Thông tin và Truyền thông là đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh;

- Phối hợp với Sở Thông tin và Truyền thông chủ trì, phối hợp với Văn phòng Ủy ban nhân dân tỉnh, Công an tỉnh và 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 UBND tỉnh đối với các cơ quan Nhà nước trong tỉnh;

Đầu mối liên hệ trực tiếp đảm bảo an toàn thông tin của Ban Dân tộc là Thanh tra và Văn phòng Ban. Khi xảy ra sự cố, tùy theo mức độ đơn vị phối hợp yêu cầu trợ giúp hoặc hướng dẫn xử lý, ứng cứu các sự cố an toàn thông tin mạng.

3. Bảo đảm nguồn nhân lực

3.1. Tuyển dụng

* Yêu cầu: Có quy định về tuyển dụng và điều kiện tuyển dụng.

* Phương án thực hiện Quy định về tuyển dụng và điều kiện tuyển dụng cán bộ:

- Quy định cán bộ được tuyển dụng 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 tuyển dụng.

- Xây dựng quy trình tuyển dụng cán bộ và điều kiện tuyển dụng cán bộ.

3.2. Trong quá trình làm việc

* Yêu cầu: Có quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc.

* Phương án thực hiện Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc:

- Quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc được quy định tại Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành

Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.

- Trách nhiệm bảo đảm an toàn thông tin đối với công chức trong cơ quan:

- Công chức sử dụng trong mạng nội bộ có trách nhiệm đảm bảo an toàn thông tin (ATTT) đối với từng vị trí công việc.

- Bộ phận hoặc cá nhân 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.

3.3. Chấm dứt hoặc thay đổi công việc

* Yêu cầu: Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc

* Phương án thực hiện Quy định đối với cán bộ, công chức, viên chức nghỉ hoặc thay đổi công việc:

- Công chức, viên chức nghỉ hoặc thay đổi công việc phải thu hồi 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 cơ quan.

- Cán bộ quản trị phải xóa bỏ, vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.

- Cán bộ nghỉ hoặc thay đổi công việc phải có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.

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

Thiết kế an toàn hệ thống thông tin: Có sơ đồ logic và sơ đồ vật lý mạng nội bộ mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành hệ thống thông tin.

5. Quản lý vận hành hệ thống thông tin

5.1. Quản lý an toàn mạng

* Yêu cầu: Có quy định về quản lý an toàn mạng

* Phương án thực hiện: Quy định về 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.

5.2. Quản lý an toàn dữ liệu

* Yêu cầu: Có quy định về quản lý an toàn dữ liệu

* Phương án thực hiện: Có quy định về quản lý an toàn dữ liệu, trang bị phần mềm diệt virus bản quyền đủ mạnh để bảo vệ hệ thống thông tin:

- Máy trạm trong hệ thống mạng nội bộ cài đặt:

+ Phần mềm diệt virus Bkav Pro thiết lập hệ thống giám sát thời gian thực, ghi nhận toàn bộ các đặc điểm, dấu hiệu, hành vi bất thường của các ứng dụng, file thực thi trên hệ thống máy tính. Trí tuệ nhân tạo tích hợp trong Bkav Pro sẽ tổng hợp các dữ liệu được ghi nhận, phân tích và chỉ ra các mối nguy hiểm người sử dụng có thể gặp phải như bị xóa dữ liệu, bị theo dõi bởi phần mềm gián điệp hay bị mất cắp tài khoản… từ đó phát lệnh xử lý, ngăn chặn và tiêu diệt mã độc.

5.3. Quản lý sự cố an toàn thông tin

* Yêu cầu: Có quy định về quản lý sự cố an toàn thông tin

* Phương án thực hiện: Quy định về quản lý sự cố an toàn thông tin:

- Thực hiện theo Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.

- Thực hiện tiếp nhận và xử lý sự cố theo Chương II/ Điều 8 Quy chế số 1195/QĐ-UBND ngày 15/8/2017 của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Bắc Kạn về ban hành quy chế hoạt đông của Đội ứng cứu sự cố mạng máy tính tỉnh Bắc Kạn.

5.4. Quản lý an toàn người sử dụng đầu cuối

* Yêu cầu: Có quy định về quản lý an toàn người sử dụng đầu cuối

* Phương án thực hiện: Quy định về quản lý an toàn người sử dụng đầu cuối:

- Cán bộ sử dụng tài nguyên mạng 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.

- 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 phòng Công nghệ thông tin để kịp thời ngăn chặn và xử lý.

II. Thuyết minh phương án bảo đảm an toàn thông tin đáp ứng các yêu cầu an toàn cơ bản về kỹ thuật

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống

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

- Vùng mạng nội bộ: Cung cấp các kết nối mạng cho các máy trạm và các thiết bị đầu cuối và các thiết bị khác của người dùng vào hệ thống.

b) Phương án bảo đảm an toàn thông tin

- Vùng mạng biên: Router có sử dụng firewall (tường lửa) do nhà mạng VNPT cung cấp.

- Các máy trạm trong vùng mạng nội bộ được cài đặt:

+ Phần mềm diệt virus Bkav Pro thiết lập hệ thống giám sát thời gian thực, ghi nhận toàn bộ các đặc điểm, dấu hiệu, hành vi bất thường của các ứng dụng, file thực thi trên hệ thống máy tính, giúp ngăn chặn mọi nguy cơ trên Internet, diệt virus, chống phần mềm gián điệp, bảo vệ dữ liệu, bảo vệ mật khẩu, …

1.2. 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 thông qua Modem.

- 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 thông qua Modem.

- Thiết lập giới hạn thời gian chờ để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng được thiết lập trên Modem.

- Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn.

1.3. 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, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức.

1.4. Nhật ký hệ thống

- Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên máy tính vùng mạng nội bộ.

- Lưu trữ và quản lý tập trung nhật ký hệ thống.

1.5. Phòng chống xâm nhập, phần mềm độc hại trên môi trường mạng

- Có phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống.

- Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng.

- Sử dụng thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên máy tính vùng mạng nội bộ và Router/Modem.

1.6. Bảo vệ thiết bị hệ thống

- Hệ thống đảm bảo an toàn, an ninh lưu trữ và đảm bảo các tiêu chuẩn an toàn về nguồn điện…

- Cấu hình chức năng xác thực trên các thiết bị của hệ thống để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa trên Router/Modem.

- 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.

1.7. Phòng chống phần mềm độc hại trên môi trường mạng

- Có phương án phòng chống phần mềm độc hại trên môi trường mạng, thực hiện theo Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.

- Các máy trạm trong vùng mạng nội bộ được cài đặt các phần mềm diệt virus bản quyền đủ mạnh để phát hiện, ngăn chặn các mối nghi ngờ tấn công từ bên ngoài.

2. Bảo đảm an toàn dữ liệu

2.1. Nguyên vẹn dữ liệu

Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn

2.2. Bảo mật dữ liệu

Lưu trữ có mã hóa các thông tin, dữ liệu trên hệ thống lưu trữ phương tiện lưu trữ, dữ liệu được nén và được lưu trữ trên các thiết bị như: USB; ổ cứng di động.

2.3. Sao lưu dự phòng

- Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

- Phân loại và quản lý các dữ liệu được lưu trữ theo từng loại nhóm thông tin được gán nhãn khác nhau

- Lưu trữ trên ổ cứng di cộng; USB để sao lưu dự phòng

Đối với các yêu cầu kỹ thuật chưa đáp ứng yêu cầu an toàn cơ bản trong Thuyết minh này, Đơn vị vận hành sẽ triển khai nâng cấp, thiết lập cấu hình hệ thống để đáp ứng yêu cầu trong vòng 18 tháng, kể từ khi HSĐXCĐ được phê duyệt.

Trên cơ sở đó, thuyết minh phương án bảo đảm an toàn thông tin cho Hệ thống 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 (Ban Dân tộc đã ban hành Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn)

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	Trước khi ban hành Quy chế đảm bảo an toàn thông tin của đơn vị, dự thảo quy chế được gửi xin ý kiến đối với toàn thể cán bộ, công chức đơn vị. Tại mục 3, Điều 12, Chương 3 Quyết định số 100/QĐ-BDT ngày 26/10/2020 của Ban Dân tộc quy định "trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc khó khăn, vướng mắc cần phản ánh kịp thời về Thanh tra và Văn phòng để tổng hợp báo cáo Trưởng Ban xem xét quyết định điều chỉnh, bổ sung cho phù hợp"

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	Đã đáp ứng
Phương án	Tại mục 3, Điều 12, Chương 3 Quyết định số 100/QĐ-BDT ngày 26/10/2020 của Ban Dân tộc quy định "trong quá trình thực hiện, nếu có vấn đề phát sinh hoặc khó khăn, vướng mắc cần phản ánh kịp thời về Thanh tra và Văn phòng để tổng hợp báo cáo Trưởng

	Ban xem xét quyết định điều chỉnh, bổ sung cho phù hợp”

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	Đã đáp ứng Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Đơn vị đã giao bộ phận Thanh tra và Văn phòng chủ trì tham mưu thực hiện các nội dung về an toàn thông tin của đơn vị

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

2.2.1. 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	Đơn vị đang sửa đổi, bổ sung Thông báo phân công nhiệm vụ các Phòng thuộc Ban Dân tộc, theo đó bổ sung nội dung phân công đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin
Phương án	Đơn vị đã giao bộ phận Thanh tra và Văn phòng là đầu mối liên hệ, phối hợp với Sở Thông tin và Truyền thông và các cơ quan, tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng

2.2.2. 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	Đã đáp ứng
Phương án	Đơn vị đã giao bộ phận Thanh tra và Văn phòng làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông

	tin của Hệ thống thông tin.

2.2.3. 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 Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	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 Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Tại Quyết định số 2309/QĐ-UBND ngày 29/12/2017 của UBND tỉnh phê duyệt Bản mô tả công việc và khung năng lực của vị trí việc làm thuộc Ban Dân tộc tỉnh Bắc Kạn đã quy định về tuyển dụng và điều kiện tuyển dụng công chức đối với vị trí công nghệ thông tin.

3.2. Trong quá trình làm việc 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 Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.

Phương án	Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn quy định về việc thực hiện bảo đảm an toàn thông tin trong quá trình làm việc: 1. Bảo mật số liệu: CB, CC, NLĐ phải có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính.Việc chia sẻ dữ liệu trên mạng do bộ phận quản trị mạng thực hiện theo quyết định của Trưởng Ban Dân tộc và theo phân cấp sử dụng tài nguyên mạng. 2. Bảo mật truy cập: Các chương trình ứng dụng, phân chia sử dụng trên máy tính phải được đặt mật khẩu, mã khoá bảo mật. 3. Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Bộ phận quản trị mạng có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập và có biện pháp xử lý kịp thời. 4. An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, CB, CC, NLĐ phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân. 5. Phòng, chống virus: CC, CC, NLĐ có trách nhiệm tuân thủ các biện pháp phòng và chống virus cho máy tính, đảm bảo an toàn dữ liệu thuộc cá nhân quản lý. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài đều phải được quét, diệt virus mỗi khi đưa vào máy. Những máy tính phát hiện có virus phải được tách khỏi mạng về mặt vật lý để tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các link liên kết không rõ ràng; không click vào các link, tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

3.3. 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 Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng

	công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	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.

3.4. Chấm dứt hoặc thay đổi công việc

a) 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.

Yêu cầu	Có quy định đối với cán bộ nghỉ hoặc thay đổi công việc
Hiện trạng	Đáp ứng một phần Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Bổ sung quy định đối với cán bộ nghỉ hoặc thay đổi công việc vào Quy chế đảm bảo an toàn thông tin của đơn vị

b) 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.

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 một phần
Phương án	Bổ sung quy trình vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc vào Quy chế đảm bảo an toàn thông tin của đơn vị

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

4.1. Thiết kế an toàn hệ thống thông tin

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 (Quy định tại Điều 5, Quyết định số 100/QĐ-BDT ngày 26/10/2020 của Ban Dân tộc)
Phương án	Tại Điều 5, Quyết định số 100/QĐ-BDT ngày 26/10/2020 của Ban Dân tộc quy định: 1. Thanh tra và Văn phòng có trách nhiệm cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại Ban; Nghiên cứu, đề xuất, nâng cấp công nghệ, phần mềm theo định hướng quản lý nhà nước của ngành và tuân theo quy định của Nhà nước. 2. Phòng Chính sách tuyên truyền và Kế hoạch tổng hợp và toàn thể CB, CC, NLĐ có trách nhiệm phối hợp với Thanh tra và Văn phòng trong quá trình triển khai, khai thác và sử dụng phần mềm.

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 *(Tại hồ sơ đề xuất cấp độ an toàn thông tin này đã mô tả thiết kế và các thành phần của hệ thống thông tin).*

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 *(Tại hồ sơ đề xuất cấp độ an toàn thông tin này đã mô tả phương án bảo đảm an toàn thông tin theo cấp độ)*

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 Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.

Phương án	Thực hiện quy định tại Điều 5, Chương II, Quyết định số 100/QĐ-BDT ngày 26/10/2020 của Ban Dân tộc tỉnh Bắc Kạn quy định: "Thanh tra và Văn phòng, Ban Dân tộc có trách nhiệm cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại Ban; Nghiên cứu, đề xuất, nâng cấp công nghệ, phần mềm theo định hướng quản lý nhà nước của ngành và tuân theo quy định của Nhà nước"

e) 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	Đáp ứng một phần Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Bổ sung 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 và Quy chế đảm bảo an toàn thông tin của đơn vị

f) Phát triển phần mềm thuê khoán:

- 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 Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Thực hiện theo QĐ số 22/2021/QĐ-UBND ngày 28/12/2021 của UBND tỉnh về việc ban hành quy chế ATTT mạng trong cơ quan nhà nước tỉnh Bắc Kạn năm 2021: 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.

- 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	Đáp ứng một phần Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Bổ sung quy định yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm vào Quy chế đảm bảo an toàn thông tin của đơn vị

g) Thử nghiệm và nghiệm thu hệ thống

- 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 một phần Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Bổ sung quy định đối với việc thử nghiệm và nghiệm thu hệ thống vào Quy chế đảm bảo an toàn thông tin của đơn vị.

- 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 một phần Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Bổ sung quy trình thử nghiệm và nghiệm thu hệ thống vào Quy chế đảm bảo an toàn thông tin của đơn vị

- 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 Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Giao Thanh tra và Văn phòng Ban Dân tộc chủ trì, phối hợp với Phòng Chính sách tuyên truyền và Kế hoạch tổng hợp thực hiện thử nghiệm và nghiệm thu hệ thống.

5. Quản lý vận hành hệ thống thông tin

5.1. Quản lý an toàn mạng

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn mạng. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế an toàn thông tin của đơn vị.

5.2. 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 *(Quy định tại Điều 5, Quyết định số 100/QĐ-BDT ngày 26/10/2020)*
Phương án	Điều 5, Quyết định số 100/QĐ-BDT ngày 26/10/2020 của Ban Dân tộc quy định: 1. Thanh tra và Văn phòng có trách nhiệm cài đặt, quản lý các phần mềm hệ thống và phần mềm ứng dụng trong hệ thống mạng máy tính tại Ban; Nghiên cứu, đề xuất, nâng cấp công nghệ, phần mềm theo định hướng quản lý nhà nước của ngành và tuân theo quy định của Nhà nước. 2. Phòng Chính sách tuyên truyền và Kế hoạch tổng hợp và toàn thể CB, CC, NLĐ có trách nhiệm phối hợp với Thanh tra và Văn phòng trong quá trình triển khai, khai thác và sử dụng phần mềm.

5.3. 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 một phần Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Thực hiện theo QĐ số 22/2021/QĐ-UBND ngày 28/12/2021 của UBND tỉnh về việc ban hành quy chế ATTT mạng trong cơ quan nhà nước tỉnh Bắc Kạn năm 2021: Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, ảnh hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

5.4. Truy cập và quản lý cấu hình hệ thống

Yêu cầu	Truy cập và quản lý cấu hình hệ thống
Hiện trạng	Đáp ứng Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Thực hiện theo QĐ số 22/2021/QĐ-UBND ngày 28/12/2021 của UBND tỉnh về việc ban hành quy chế ATTT mạng trong cơ quan nhà nước tỉnh Bắc Kạn năm 2021: Cán bộ quản lý, nhân viên vận hành truy cập, khai thác thông tin tại Trung tâm dữ liệu theo trách nhiệm và phân quyền được quy định; việc khai thác thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

5.5. Quản lý an toàn máy chủ và ứng dụng

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn máy chủ và ứng dụng. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

5.5.1 Chính sách, quy trình quản lý an toàn máy chủ và ứng dụng bao gồm:

a) 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 một phần
Phương án	Quản lý, vận hành hoạt động bình thường của hệ thống máy chủ và dịch vụ: a) Bảo đảm cho hệ điều hành, phần mềm cài đặt trên máy chủ hoạt động liên tục, ổn định và an toàn. b) Thường xuyên kiểm tra cấu hình, các file nhật ký hoạt động của hệ điều hành, phần mềm nhằm kịp thời phát hiện và xử lý những sự cố nếu có. c) Quản lý các thay đổi cấu hình kỹ thuật của hệ điều hành, phần mềm. d) Thường xuyên cập nhật các bản vá lỗi hệ điều hành, phần mềm từ nhà cung cấp. đ) Loại bỏ các thành phần của hệ điều hành, phần mềm không cần thiết hoặc không còn nhu cầu sử dụng. e) Các bản quyền phần mềm cần được thống kê, quản lý thời gian hạn phục vụ cho việc gia hạn.

b) Truy cập mạng của máy chủ

Yêu cầu	Có quy định quản lý truy cập mạng của máy chủ
Hiện trạng	Đáp ứng một phần thực hiện theo QĐ số 22/2021/QĐ-UBND ngày 28/12/2021 của UBND tỉnh về việc ban hành quy chế ATTT mạng trong cơ quan nhà nước tỉnh Bắc Kạn năm 2021
Phương án	Truy cập mạng của máy chủ: Bảo đảm các kết nối mạng trên máy chủ hoạt động liên tục, ổn định và an toàn. Cấu hình, kiểm soát các kết nối, các cổng dịch vụ từ bên trong đi ra cũng nhưng bên ngoài vào hệ thống.

c) 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	Đáp ứng một phần thực hiện theo QĐ số 22/2021/QĐ-UBND ngày 28/12/2021 của UBND tỉnh về việc ban hành quy chế ATTT mạng trong cơ quan nhà nước tỉnh Bắc Kạn năm 2021
Phương án	Truy cập và quản trị máy chủ và ứng dụng: a) Thay đổi các tài khoản, mật khẩu mặc định ngay khi đưa hệ điều hành, phần mềm vào sử dụng. b) Cấp quyền quản lý truy cập của người sử dụng trên máy chủ cài đặt hệ điều hành. c) Toàn bộ máy chủ và thiết bị công nghệ thông tin không phải máy tính ngoại trừ các hệ thống bắt buộc phải có giao tiếp với Internet (các hệ thống phục vụ truy cập Internet; cung cấp giao diện ra Internet của trang tin điện tử, dịch vụ công, thư điện tử; phục vụ cập nhật bản vá hệ điều hành, mẫu mã độc, mẫu điểm yếu, mẫu tấn công) không được kết nối Internet.

5.6. 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	Đáp ứng một phần Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Bổ sung vào Quy chế an toàn thông tin của đơn vị các quy định về cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố: Triển khai hệ thống/phương tiện lưu trữ độc lập với hệ thống lưu trữ trên các máy chủ dịch vụ để sao lưu dự phòng; phân loại và quản lý thông tin, dữ liệu được lưu trữ theo từng loại/nhóm thông tin được gán nhãn khác nhau; thực hiện sao lưu, dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ.

5.7. Quản lý an toàn dữ liệu

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn dữ liệu. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

5.8. 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	Đáp ứng một phần Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Bổ sung vào quy chế đảm bảo an toàn thông tin của đơn vị

5.9. 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	Bổ sung vào Quy chế đảm bảo an toàn thông tin của đơn vị

5.10. Quản lý sự cố an toàn thông tin

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý sự cố an toàn thông tin. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế và ban hành trong vòng 06 tháng sau khi HSĐXCĐ được phê duyệt.

5.11. Phân nhóm sự cố an toàn thông tin mạng

Yêu cầu	Có quy định về phân nhóm sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng một phần

Phương án	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/QĐ-TTg, trong đó quy định rõ về phân nhóm sự cố an toàn thông tin mạng

5.12. Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng

Yêu cầu	Có phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng một phần
Phương án	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/QĐ-TTg, trong đó quy định rõ phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng

5.13. Kế hoạch ứng phó sự cố an toàn thông tin mạng

Yêu cầu	Xây dựng kế hoạch ứng phó sự cố an toàn thông tin mạng
Hiện trạng	Đáp ứng một phần Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Xây dựng và triển khai kế hoạch ứng phó sự cố an toàn thông tin theo quy định tại Điều 16, Quyết định số 05/2017/QĐ-TTg.

5.14. Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin

Yêu cầu	Có quy định về quản lý giám sát, phát hiện và cảnh báo sự cố an toàn thông tin
Hiện trạng	Đã đáp ứng
Phương án	Tại Mục 4, Điều 8, Quyết định số 100/QĐ-BDT ngày 26/10/2020 của Ban Dân tộc: Đảm bảo công tác giám sát thường xuyên để kịp thời phát hiện và ngăn chặn các hành vi tấn công mạng gây mất an toàn thông tin.

5.15. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường

Yêu cầu	Có quy trình ứng cứu sự cố an toàn thông tin mạng thông thường
Hiện trạng	Đáp ứng một phần
Phương án	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/QĐ-TTg.

5.16. Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng

Yêu cầu	Có quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng
Hiện trạng	Đáp ứng một phần
Phương án	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/QĐ-TTg.

5.17. Cơ chế 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	Có quy định về cơ chế 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
Hiện trạng	Đáp ứng một phần
Phương án	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

5.18. Quản lý an toàn người sử dụng đầu cuối

Dự thảo quy chế đưa ra quy định về chính sách, chưa đáp ứng yêu cầu về quy trình quản lý an toàn người sử dụng đầu cuối. Đơn vị vận hành sẽ xây dựng và bổ sung vào quy chế an toàn thông tin của đơn vị.

5.19. Quản lý truy cập, sử dụng tài nguyên nội bộ

Yêu cầu	Có quy định về quản lý truy cập, sử dụng tài nguyên nội bộ

Hiện trạng	Đáp ứng một phần
Phương án	Bổ sung vào Quy chế đảm bảo an toàn thông tin của đơn vị

5.20. Quản lý truy cập mạng và tài nguyên trên Internet

Yêu cầu	Có quy định về quản lý truy cập mạng và tài nguyên trên Internet
Hiện trạng	Đáp ứng Quyết định số 100/QĐ-BDT ngày 26/10/2020 ban hành Quy chế đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của Ban Dân tộc tỉnh Bắc Kạn.
Phương án	Tại điều 10, Điều 11, Quyết định số 100/QD-BDT ngày 26/10/2020 của Ban Dân tộc quy định các nội dung quản lý truy cập mạng và tài nguyên Internet: **Điều 10:** Trong trao đổi thông tin, dữ liệu phục vụ công việc, cơ quan, cán bộ công chức và người lao động phải sử dụng hệ thống thông tin do tỉnh Bắc Kạn cấp (@backan.gov.vn), phần mềm quản lý văn bản và hồ sơ công việc. Hạn chế việc sử dụng các phương tiện trao đổi thông tin dữ liệu, hệ thống thư điện tử công cộng, mạng xã hội trên Internet trong hoạt động của đơn vị. **Điều 11. Những điều không được làm** 1. Không được lợi dụng việc sử dụng Internet nhằm mục đích: Chống lại nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội; kích động bạo lực, đồi trụy, tệ nạn xã hội, mê tín dị đoan; phá hoại thuần phong mỹ tục của dân tộc. 2. Không được tiết lộ bí mật nhà nước và các bí mật khác đã được pháp luật quy định. 3. Không được chơi các trò chơi trực tuyến (game online) hoặc các trò chơi khác trên Internet trong giờ làm việc. 4. Không được truy cập hoặc tải các trang website có nội dung đồi trụy, phản động, các chương trình không rõ nguồn gốc, các thông tin quảng cáo hấp dẫn. 5. Khi sử dụng hệ thống thư điện tử (email) không được kích

	chuột vào bất cứ thư điện tử, tệp đính kèm, đường link, thư rác, thư quảng cáo nào không rõ nguồn gốc và không xác định được người gửi. 6. Không sử dụng thư điện tử công vụ để đăng ký vào mạng xã hội, diễn đàn và các trang thông tin điện tử công cộng khác.

PHỤ LỤC II
THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÀNH PHẦN CẤP ĐỘ 2

Hệ thống thông tin được đề xuất là cấp độ 2. Do đó, các thành phần trong hệ thống như hạ tầng mạng, hệ thống lưu trữ…được thuyết minh phương án đáp ứng yêu cầu cấp độ 2 như sau:

1. Bảo đảm an toàn mạng

1.1. Thiết kế hệ thống

a) Các vùng mạng trong hệ thống:

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Vùng mạng nội bộ	N/A	Hệ thống không sử dụng vùng mạng này
2	Vùng mạng biên	Có	Kết nối hệ thống với mạng Internet và mạng diện rộng
3	Vùng DMZ	Có	Đặt máy chủ WEBAPP, cho phép truy cập trực tiếp từ các mạng bên ngoài và mạng Internet.
4	Vùng máy chủ nội bộ	Có	Là vùng đặt máy chủ cơ sở dữ liệu.

b) Phương án bảo đảm an toàn thông tin

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	Sử dụng Tường lửa Generic Firewall có tích hợp chức năng VPN để quản lý truy cập, quản trị hệ thống từ xa an toàn.
2	Phương án quản lý	Có	Sử dụng Tường lửa Generic Firewall có

	truy cập giữa các vùng mạng và phòng chống xâm nhập		tích hợp chức năng IPS để quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập.
3	Phương án dự phòng cho các thiết bị mạng chính	Có	Các thiết bị mạng chính: Router, Firewall, Switch đều có thiết bị dự phòng

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 sử dụng Tường lửa Generic Firewall có tích hợp chức năng VPN 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.
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 Generic Firewall được thiết lập chỉ cho phép 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
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) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng trên Tường lửa Generic Firewall và ngắt phiên kết nối VPN khi người dùng không thao tác sử dụng trong 1 khoảng thời gian

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	Có	Chính sách kiểm soát truy cập từ các vùng mạng trong hệ thống đi ra các mạng bên ngoài và mạng Internet được thiết lập trên Tường lửa Generic Firewall

1.4. Nhật ký hệ thống

Yêu cầu / **Thiết bị**	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
Router: Draytek Vigor 2912F	+	+
Generic Firewall	+	+
Swith TP-Link TL-SG1024D	+	+

1.5. Phòng chống xâm nhập

STT	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 Generic Firewall có tích hợp chức năng IPS để bảo vệ các vùng mạng trong hệ thống
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 Generic Firewall.

1.6. Bảo vệ thiết bị hệ thống

Yêu cầu / **Thiết bị**	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
Router: Draytek Vigor 2912F	+	+	+
Generic Firewall	+	+	+
Swith TP-Link TL-SG1024D	+	+	+

2. Bảo đảm an toàn máy chủ

2.1. Xác thực

Yêu cầu	Thiết lập chính sách xác thực trên máy chủ	Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa	Thiết lập chính sách mật khẩu an toàn: Yêu cầu thay đổi mật khẩu mặc định; Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự; Thiết lập thời gian yêu cầu thay đổi mật khẩu; Thiết lập thời gian mật khẩu hợp lệ

2.2. Kiểm soát truy cập

Yêu cầu	Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa	Thiết lập giới hạn thời gian chờ (timeout)

2.3. Nhật ký hệ thống

Yêu cầu	Thiết lập lập chức năng ghi nhật ký hệ	Đồng bộ thời gian giữa máy chủ với máy chủ thời gian	Lưu nhật ký hệ thống trong khoảng thời gian

	thống trên các máy chủ		tối thiểu là 01 tháng

2.4. Phòng chống xâm nhập

Yêu cầu	Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ	Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ	Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng	Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng
	+	+	+	+
	+	+	+	+

2.5. Phòng chống phần mềm độc hại

Yêu cầu	Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật	Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt

2.6. Xử lý máy chủ khi chuyển giao

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	Đáp ứng	Hiện tại chưa có phương án chuyển giao cho đơn vị sử dụng. Sẽ có phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng

3. Bảo đảm an toàn ứng dụng

3.1. 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	Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định
Ứng dụng				
Hệ thống ...	+	+	+	+

3.2. 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	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa
Ứng dụng			
Hệ thống thông tin nội bộ và phần mềm ứng dụng	+	+	+

3.3. 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; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng.	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng
Ứng dụng		

Hệ thống thông tin nội bộ và phần mềm ứng dụng	+	+

3.4. An toàn ứng dụng và mã nguồn

Yêu cầu	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
Ứng dụng	
Hệ thống quản lý văn bản nội bộ	+
Hệ thống thông tin nội bộ và phần mềm ứng dụng	+

4. Bảo đảm an toàn dữ liệu

4.1 Bảo mật dữ liệu

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	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	Có	Dữ liệu được nén và được lưu trữ mã hóa sử dụng EAS 256

4.2 Sao lưu dự phòng

STT	Yêu cầu	P/A	Ghi chú/Mô tả
1	Thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ	Có	Có thực hiện sao lưu dự phòng các thông tin, dữ liệu cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ trên ổ cứng di động

PHỤ LỤC III
THUYẾT MINH PHƯƠNG ÁN KỸ THUẬT ĐỐI VỚI HỆ THỐNG THÔNG TIN NỘI BỘ CẤP ĐỘ II

1. Bảo đảm an toàn ứng dụng

1.1 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			
Hệ thống thông tin nội bộ và phần mềm ứng dụng	+	+	+

1.2. 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	Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa
Ứng dụng			
Hệ thống thông tin nội bộ và phần mềm ứng dụng	+	+	+

1.3. 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; (3) Thông tin các lỗi phát sinh trong quá trình hoạt động (4) Thông tin thay đổi cấu hình ứng dụng.	Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 01 tháng
Ứng dụng		
Hệ thống quản lý văn bản nội bộ	+	+

Hệ thống thông tin nội bộ và phần mềm ứng dụng	+	+

1.4. An toàn ứng dụng và mã nguồn

Yêu cầu	Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý
Ứng dụng	
Hệ thống quản lý văn bản nội bộ	+
Hệ thống thông tin nội bộ và phần mềm ứng dụng	+