ỦY BAN NHÂN DÂN TỈNH YÊN BÁI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 34 /2022/QĐ-UBND	*Yên Bái, ngày 14 tháng 12 năm 2022*

QUYẾT ĐỊNH
Ban hành Quy chế quản lý, vận hành Trung tâm Giám sát an toàn không gian mạng tỉnh Yên Bái

ỦY BAN NHÂN DÂN TỈNH YÊN BÁI

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015; Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22 tháng 11 năm 2019;

Căn cứ Luật Ban hành văn bản quy phạm pháp luật ngày 22 tháng 6 năm 2015; Căn cứ Luật sửa đổi, bổ sung một số điều của Luật Ban hành văn bản quy phạm pháp luật ngày 18 tháng 6 năm 2020;

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

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 15 tháng 11 năm 2018;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Nghị định số 34/2016/NĐ-CP ngày 14 tháng 5 năm 2016 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Ban hành văn bản quy phạm pháp luật;

Căn cứ Nghị định số 154/2020/NĐ-CP ngày 31 tháng 12 năm 2020 của Chính phủ sửa đổi, bổ sung một số điều của Nghị định số 34/2016/NĐ-CP ngày 14 tháng 5 năm 2016 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Ban hành văn bản quy phạm pháp luật;

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 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 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;

Theo đề nghị của Chánh Văn phòng Ủy ban nhân dân tỉnh tại Tờ trình số 1092/TTr-VP ngày 05 tháng 12 năm 2022.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế quản lý, vận hành Trung tâm Giám sát an toàn không gian mạng tỉnh Yên Bái.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày 25 tháng 12 năm 2022.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Thủ trưởng các ban, sở, ngành của tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố; các cơ quan, đơn vị, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục kiểm tra văn bản (Bộ Tư pháp);
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- Đoàn Đại biểu Quốc hội tỉnh;
- Chủ tịch, các Phó Chủ tịch UBND tỉnh;
- Chánh, các Phó Chánh VP UBND tỉnh;
- Trung tâm điều hành thông minh tỉnh;
- Trung tâm Chuyển đổi số;
- Lưu: VT, NC, HC-TC, VX.

TM. ỦY BAN NHÂN DÂN TỈNH
CHỦ TỊCH

Trần Huy Tuấn

ỦY BAN NHÂN DÂN TỈNH YÊN BÁI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ

Quản lý, vận hành Trung tâm Giám sát an toàn không gian mạng tỉnh Yên Bái

(Kèm theo Quyết định số 34/2022/QĐ-UBND ngày 14 tháng 12 năm 2022 của Ủy ban nhân dân tỉnh Yên Bái)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định việc quản lý, vận hành Trung tâm Giám sát an toàn không gian mạng tỉnh Yên Bái (gọi tắt là Trung tâm SOC tỉnh Yên Bái).

2. Đối tượng áp dụng: Quy chế này áp dụng với các cơ quan, đơn vị trên địa bàn tỉnh và các tổ chức, cá nhân có liên quan tham gia quản lý, vận hành Trung tâm SOC tỉnh Yên Bái.

Điều 2. Giải thích từ ngữ

Trong quy chế này, các từ ngữ dưới đây được hiểu như sau:

1. Trung tâm SOC tỉnh Yên Bái là một hệ thống công cụ phần cứng, phần mềm được cài đặt tại Trung tâm tích hợp dữ liệu tỉnh và tại các sở, ban, ngành và UBND các huyện, thị xã, thành phố trong tỉnh có kết nối tới Trung tâm Giám sát an toàn không gian mạng quốc gia tạo thành hệ thống đồng bộ, thống nhất đảm bảo an toàn thông tin của tỉnh phục vụ phát triển Chính quyền điện tử, đô thị thông minh và các hoạt động chuyển đổi số của tỉnh Yên Bái.

2. Mạng là môi trường trong đó thông tin được cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông qua mạng viễn thông và mạng máy tính.

3. Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xử lý, lưu trữ và trao đổi thông tin trên mạng.

4. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

Điều 3. Chức năng và các thành phần cơ bản của Trung tâm SOC tỉnh Yên Bái

1. Các chức năng cơ bản của Trung tâm SOC tỉnh Yên Bái bao gồm:

a) Chức năng phòng, chống tấn công từ chối dịch vụ (DoS/DDoS Datacenter).

b) Chức năng chống tấn công cho các ứng dụng trên nền tảng WEB (WAF) Datacenter.

c) Chức năng Tường lửa bảo vệ lớp mạng (Network-base Firewall).

d) Chức năng giám sát an toàn thông tin tập trung (SOC) với đầy đủ các chức năng, hỗ trợ chia sẻ, kết nối với Trung tâm giám sát an toàn không gian mạng quốc gia (NCSC) và các hệ thống giám sát, quản lý an toàn thông tin tập trung khác.

đ) Chức năng kết nối mạng riêng ảo (VPN) tạo kênh kết nối riêng giữa Trung tâm SOC tỉnh đến Hệ thống mạng của các sở, ban, ngành và Ủy ban nhân dân (UBND) các huyện, thị xã, thành phố trong tỉnh thông qua các thiết bị, hệ thống mạng có mã hóa đường truyền, tích hợp đa dạng các tính năng bảo đảm an toàn thông tin (mạng riêng ảo).

e) Chức năng bảo vệ máy tính cá nhân/máy chủ (PC/Laptop/Server Security). Với các chức năng: Chống virus, mã độc hại; Phát hiện và ngăn chặn các loại tấn công có chủ đích (ATP) đến thiết bị đầu cuối; Tường lửa, phát hiện, chống tấn công (IPS/IDS); Kiểm soát truy nhập; Giám sát hoạt động của thiết bị; hỗ trợ cập nhật bản vá phần mềm; Hỗ trợ mã hóa dữ liệu, sao lưu dữ liệu trên thiết bị đầu cuối phần mềm

2. Các thành phần cơ bản của Trung tâm SOC tỉnh Yên Bái

a) Công nghệ gồm các phương án, giải pháp kỹ thuật được sử dụng để bảo đảm việc giám sát an toàn thông tin đáp ứng các yêu cầu về kỹ thuật và tính hiệu quả, với các thành phần sau: Quản lý, phân tích sự kiện an toàn thông tin (SIEM); Phòng, chống mã độc (Anti-Virus); Phát hiện và phản ứng sự cố an toàn thông tin trên thiết bị đầu cuối (EDR).

b) Quy trình gồm các quy định trong quy chế, chính sách bảo đảm an toàn thông tin của cơ quan, tổ chức được xây dựng để phục vụ việc quản lý, vận hành hệ thống an toàn.

c) Nhân lực của Trung tâm SOC tỉnh Yên Bái gồm: Các cán bộ chuyên trách vận hành tại Trung tâm SOC tỉnh Yên Bái; Tổ giám sát an toàn không gian mạng phục vụ Đô thị thông minh tỉnh Yên Bái và đội ngũ chuyên gia của đơn vị giám sát, bảo vệ chuyên nghiệp do tỉnh Yên Bái thuê dịch vụ giám sát, bảo vệ an toàn thông tin. Đồng thời, có sự phối hợp chặt chẽ của Đội ứng cứu xử lý sự cố an toàn thông tin mạng tỉnh Yên Bái do Sở Thông tin và Truyền thông là cơ quan thường trực.

Điều 4. Nguyên tắc quản lý và vận hành Trung tâm SOC tỉnh Yên Bái

1. Phải đảm bảo vận hành hoạt động thường xuyên, liên tục, ổn định 24 giờ trong các ngày, 7 ngày trong các tuần.

2. Chủ động theo dõi, phân tích, phòng ngừa để kịp thời phát hiện, ngăn chặn, xử lý sự cố an toàn thông tin không gian mạng. Khi phát hiện sự cố phải kịp thời thông báo đến Sở Thông tin và Truyền thông (Cơ quan thường trực Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Yên Bái) để thực hiện điều phối, ngăn chặn, xử lý.

3. Phải có sự điều phối, kết hợp chặt chẽ, hiệu quả giữa Trung tâm SOC tỉnh Yên Bái với Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh, đồng thời kết nối với Trung tâm Giám sát an toàn không gian mạng quốc gia và các đơn vị có chức năng, nhiệm vụ có liên quan.

4. Hình thức thông báo, trao đổi thông tin

Tùy vào tính chất, mức độ của sự việc, Trung tâm SOC tỉnh sử dụng các hình thức thông báo, trao đổi thông tin sau:

a) Hình thức gọi điện thoại.

b) Hình thức nhắn tin SMS.

c) Hình thức gửi qua hòm thư điện tử

d) Hình thức gửi văn bản

Chương II
QUẢN LÝ, VẬN HÀNH TRUNG TÂM GIÁM SÁT AN TOÀN KHÔNG GIAN MẠNG TỈNH YÊN BÁI

Điều 5. Giám sát, phát hiện và bảo vệ hệ thống thông tin

1. Đối tượng được giám sát, bảo vệ tại Trung tâm SOC tỉnh Yên Bái:

a) Hệ thống máy chủ của Trung tâm tích hợp dữ liệu tỉnh Yên Bái.

b) Hệ thống các phần mềm, cơ sở dữ liệu và ứng dụng tại Trung tâm tích hợp dữ liệu tỉnh Yên Bái.

c) Các hệ thống thông tin điện tử, phần mềm và cơ sở dữ liệu của các sở, ban, ngành và UBND các huyện, thị xã, thành phố của tỉnh Yên Bái.

d) Hệ thống mạng, máy tính công vụ tại các cơ quan, đơn vị trên địa bàn tỉnh được thiết lập, kết nối về Trung tâm SOC tỉnh Yên Bái.

đ) Hệ thống thông tin khác có liên quan.

2. Quy định giám sát, bảo vệ hệ thống thông tin của Trung tâm SOC tỉnh Yên Bái.

a) Việc giám sát phải được thực hiện liên tục 24 giờ trong các ngày, 7 ngày trong các tuần đối với các sự kiện từ hệ thống cần bảo vệ; giám sát màn hình cảnh báo; kiểm tra và phân loại cảnh báo; phân công xử lý, theo dõi xử lý, hoàn thành lưu trữ kết quả xử lý.

b) Xử lý sự cố an toàn thông tin: Phân tích sơ bộ nhật ký hệ thống log, các dấu hiệu tấn công, truy cập trái phép; nhận diện và xác định mức độ của sự cố; xác định các hành động cần thiết phải xử lý và phân công trách nhiệm của các thành phần tham gia xử lý (làm rõ nhiệm vụ của bộ phận chuyên trách và trách nhiệm của các cơ quan, đơn vị có liên quan); phân tích, khoanh vùng, điều tra nguyên nhân; thực hiện khắc phục sự cố.

c) Phân tích, phát hiện nguy cơ mất an toàn thông tin để thông báo đến các cơ quan, đơn vị có nguy cơ mất an toàn thông tin chủ động phòng ngừa.

Điều 6. Ứng cứu, xử lý sự cố

1. Đối với các sự cố do Trung tâm SOC tỉnh Yên Bái phát hiện, Đơn vị vận hành Trung tâm SOC tỉnh Yên Bái phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng tỉnh thực hiện điều phối hoạt động ứng cứu, xử lý sự cố theo quy trình đảm bảo nhanh chóng, chính xác, kịp thời, hiệu quả.

2. Phân loại mức độ nghiêm trọng của các sự cố

a) Mức độ sự cố thấp: Là sự cố gây ảnh hưởng cá nhân và không làm gián đoạn hay đình trệ hoạt động chính của cơ quan, đơn vị như: máy tính trạm bị nhiễm phần mềm độc hại; phần mềm hệ điều hành, các phần mềm ứng dụng cài đặt trên máy tính cá nhân phát sinh lỗi.

b) Mức độ sự cố trung bình: Là sự cố ảnh hưởng đến một nhóm người dùng nhưng không gây gián đoạn hay đình trệ hoạt động chính của đơn vị như: hệ thống mạng của 01 phòng, ban thuộc đơn vị bị ngưng hoạt động, phần mềm độc hại lây nhiễm tất cả các máy tính trạm trong 01 phòng, ban.

c) Mức độ sự cố cao: Là sự cố làm cho thiết bị, phần mềm hay hệ thống không thể sử dụng được và gây ảnh hưởng đến một trong các hoạt động chính của cơ quan như: hệ thống quản lý văn bản và điều hành, hồ sơ cấp phép, một cửa điện tử của đơn vị bị ngưng hoạt động, một số thiết bị công nghệ thông tin quan trọng (bộ chuyển mạch trung tâm, thiết bị định tuyến, thiết bị tường lửa, máy chủ quản lý tập tin chung,) bị hư hỏng.

d) Mức độ sự cố khẩn cấp: Là sự cố ảnh hưởng đến sự liên tục của nhiều hoạt động chính của cơ quan, đơn vị như: toàn bộ hệ thống thiết bị công nghệ thông tin, hệ thống cung cấp điện ngừng hoạt động, hệ thống trang thông tin điện tử bị tin tặc (hacker) tấn công, xâm nhập, thay đổi nội dung.

Điều 7. Quy trình xử lý sự cố của Trung tâm SOC tỉnh Yên Bái

1. Quy trình giám sát, bảo vệ hệ thống thông tin: Khi có sự cố hoặc nguy cơ mất an toàn thông tin xảy ra như: Hệ thống hoạt động chậm bất thường, không truy cập được hệ thống, nội dung thông tin bị thay đổi không chủ động hoặc các dấu hiệu bất thường khác thì tiến hành quy trình ứng cứu sự cố an toàn thông tin mạng theo các nội dung sau:

a) Bước 1: Ghi nhận sự cố

Hệ thống: Trong quá trình vận hành, theo dõi hệ thống phần mềm của Trung tâm SOC tỉnh Yên Bái đưa ra cảnh báo về các sự cố.

Nhân lực: Các sự cố được báo cáo bởi thành viên Tổ ứng cứu sự cố an toàn thông tin mạng tỉnh; các cơ quan, đơn vị, tổ chức hoặc cá nhân trên địa bàn tỉnh. Các sự cố đều được ghi nhận vào nhật ký xử lý sự cố đảm bảo đầy đủ, chính xác và kịp thời có sự xác nhận của các đầu mối liên quan.

b) Bước 2: Phân tích và xác nhận sự cố

Phân tích sơ bộ về sự cố, mức độ và phạm vi ảnh hưởng qua đó có thể phân loại mức độ sự cố. Đơn vị vận hành Trung tâm SOC tỉnh Yên Bái phân tích đưa ra đề xuất về biện pháp ngăn chặn tạm thời để hạn chế việc mở rộng tấn công, khai thác và làm giảm phạm vi tấn công vào hệ thống. Mức độ nghiêm trọng của sự cố được phân loại theo khoản 2, Điều 6 Quy chế này.

c) Bước 3: Thông báo

Ngay sau khi phân tích, xác nhận sự cố, Trung tâm SOC Yên Bái thực hiện thông báo đến Sở Thông tin và Truyền thông thực hiện điều phối ứng cứu an toàn thông tin, đến các cơ quan, đơn vị xảy ra sự cố, nếu cần thiết có thể yêu cầu phối hợp với các cơ quan, đơn vị liên quan cùng khắc phục.

d) Bước 4: Ngăn chặn

Đơn vị vận hành Trung tâm SOC tỉnh Yên Bái phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng tỉnh, cán bộ an toàn thông tin của các cơ quan, đơn vị trong tỉnh thực hiện phương án ngăn chặn sự lây lan sự cố hoặc trì hoãn tiến trình tấn công mạng vào hệ thống. Một số biện pháp có thể đưa ra như: cô lập thiết bị, hệ thống ra khỏi mạng hiện đang sử dụng của đơn vị; ngắt mạng hoặc dịch vụ đang gặp sự cố.

đ) Bước 5: Thu thập bằng chứng và truy tìm thủ phạm

Trung tâm SOC tỉnh Yên Bái chịu trách nhiệm thu thập các file dữ liệu có lữu trữ nhật ký hoạt động của các hệ thống, thiết bị gặp sự cố; phân tích nhật ký hoạt động và lưu giữ, bảo quản các chứng cứ số để thực hiện điều tra nguyên nhân gây ra sự cố, thủ phạm.

e) Bước 6: Xử lý nguyên nhân sự cố

Sau khi thu thập bằng chứng và phân tích đã xác định được nguyên nhân gây ra sự cố, thủ phạm, Đơn vị vận hành Trung tâm SOC tỉnh Yên Bái phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng tỉnh để thực hiện loại bỏ nguyên nhân gây ra sự cố.

Nếu nguyên nhân gây ra sự cố đã được loại bỏ, cần xem xét và đánh giá sự cố có còn tồn tại trong các hệ thống tương tự hay không.

g) Bước 7. Khôi phục

Sau khi đã loại bỏ nguyên nhân gây ra sự cố khỏi tất cả các hệ thống, Đơn vị vận hành Trung tâm SOC tỉnh Yên Bái phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng tỉnh khôi phục lại hệ thống, dịch vụ, tài nguyên và dữ liệu đã bị ảnh hưởng trong quá trình xảy ra sự cố, cần thực hiện kiểm tra, xác định tất cả dữ liệu bị mất, khôi phục dữ liệu từ bản sao lưu một cách đầy đủ. Sau khi đã thực hiện khôi phục tất cả dữ liệu bị mất, cần khởi động lại tất cả các quy trình và dịch vụ để duy trì hoạt động của cơ quan, tổ chức.

h) Bước 8. Hoạt động sau sự cố

Trung tâm SOC Yên Bái đánh giá, đề xuất các biện pháp, sản phẩm và xem xét các chính sách về an toàn thông tin để xây dựng hệ thống an toàn hơn và tránh lặp lại các sự cố tương tự xảy ra trong tương lai. Báo cáo kết quả khắc phục, xử lý sự cố đến cơ quan, đơn vị, tổ chức và cá nhân liên quan kịp thời theo quy định cụ thể tại Điều 10 của quy chế này

2. Quy trình xử lý sự cố đối với Hệ thống giám sát tại Trung tâm SOC tỉnh Yên Bái

Khi xảy ra sự cố, cần thực hiện các nội dung sau:

a) Khởi động và tắt hệ thống giám sát.

b) Thay đổi cấu hình và các thành phần của hệ thống giám sát.

c) Xử lý các sự cố liên quan đến hoạt động của hệ thống giám sát.

d) Sao lưu, dự phòng cấu hình hệ thống và nhật ký hệ thống (log) của hệ thống.

đ) Bảo trì, nâng cấp hệ thống giám sát.

e) Khôi phục hệ thống sau sự cố.

g) Trường hợp gặp sự cố nghiêm trọng, đơn vị vận hành Trung tâm SOC tỉnh không tựu xử lý được, phải báo cáo ngay cho đơn vị quản lý để kịp thời trao đổi với các đơn vị có chức năng và thẩm quyền hỗ trợ xử lý sự cố.

Điều 8. Quy định về trao đổi, cung cấp, chia sẻ thông tin nâng cao chất lượng hoạt động của hệ thống

1. Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia của Cục An toàn thông tin, Bộ Thông tin và Truyền thông, thực hiện đăng ký đầy đủ các dải địa chỉ IP public của các hệ thống thông tin trong các cơ quan nhà nước trên địa bàn tỉnh phục vụ việc theo dõi, cảnh báo các kết nối bất thường, độc hại. Đăng ký tham gia Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia do Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam, Cục An toàn thông tin, Bộ Thông tin và Truyền thông điều phối.

2. Cung cấp tình hình an toàn thông tin với đơn vị chuyên trách về an toàn thông tin là Sở Thông tin và Truyền thông; phối hợp chặt chẽ với Đội ứng cứu sự cố an toàn thông tin mạng tỉnh; phối hợp chặt chẽ với cán bộ được phân công nhiệm vụ đảm bảo an toàn thông tin của các cơ quan, đơn vị trong xử lý sự cố và đảm bảo an toàn thông tin.

Phối hợp, chia sẻ thông tin với Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao của Công an tỉnh nhằm tăng cường công tác đảm bảo an ninh mạng, an toàn thông tin và phòng, chống tội phạm sử dụng công nghệ cao.

3. Ngoài lực lượng tại chỗ, Trung tâm SOC tỉnh Yên Bái lựa chọn đơn vị có lực lượng chuyên nghiệp, đủ năng lực thực hiện giám sát, bảo vệ chuyên nghiệp để đảm bảo an toàn thông tin cho hệ thống thông tin của tỉnh cấp độ 3 trở lên.

4. Định kỳ tối thiểu 01 năm một lần được tổ chức, doanh nghiệp độc lập với đơn vị giám sát, bảo vệ chuyên nghiệp để thực hiện kiểm tra, đánh giá, rà quét, phát hiện lỗ hổng, điểm yếu, kiểm thử xâm nhập hệ thống để có biện pháp phòng ngừa, khắc phục phù hợp.

Điều 9. Quản lý danh mục hồ sơ liên quan

1. Danh sách các loại hồ sơ lưu trữ

a) Quy định về quản trị, vận hành các hệ thống.

b) Các quy trình vận hành, xử lý hệ thống.

c) Các quy trình bảo hành, bảo trì, bảo dưỡng hệ thống.

d) Hồ sơ thiết kế, thuyết minh kỹ thuật, hoàn công.

đ) Hồ sơ quản trị các hệ thống thông tin điện tử được theo dõi, giám sát.

e) Hồ sơ theo dõi xử lý sự cố.

g) Bảng thống kê danh sách thiết bị, phần mềm tại Trung tâm SOC tỉnh Yên Bái; thiết bị, phần mềm lắp đặt và cài tại các cơ quan, đơn vị, địa phương; danh sách các thiết bị hỏng, hết khấu hao sử dụng chờ thanh lý; biên bản bàn giao thiết bị cho người quản trị, người sử dụng (nếu có).

h) Tài liệu, biên bản kiểm tra, đánh giá của các cơ quan, đơn vị có liên quan.

i) Báo cáo quản trị hệ thống, nhật ký vận hành hệ thống.

k) Các hồ sơ, tài liệu kỹ thuật khác.

2. Hồ sơ phải được lưu bằng văn bản, tập tin bản mềm trên máy tính hoặc phần mềm quản lý điều hành và phải được cập nhật khi có sự thay đổi.

Điều 10. Quy định về báo cáo

1. Đơn vị vận hành phải có báo cáo định kỳ bằng văn bản hàng tháng, hàng quý, hàng năm về kết quả giám sát của Trung tâm SOC tỉnh Yên Bái về kết quả giám sát, phát hiện và xử lý các cảnh bảo và sự cố.

2. Báo cáo đột xuất là báo cáo bằng điện thoại cho thường trực Đội ứng cứu sự cố an toàn thông tin mạng tỉnh ngay sau khi phát hiện và xử lý những vấn đề có nguy cơ mất an toàn thông tin cao có khả năng gây hậu quả nghiêm trọng, sau đó báo cáo bằng văn bản gửi về Sở Thông tin và Truyền thông.

3. Báo cáo gửi về đơn vị quản lý và gửi Sở Thông tin và Truyền thông để tổng hợp báo cáo Ủy ban nhân dân tỉnh và Bộ Thông tin và Truyền thông.

4. Thông báo đến các cơ quan, đơn vị về nguy cơ mất an toàn thông tin, các lỗi, lỗ hổng bảo mật, nguy cơ mất an toàn thông tin được phát hiện trên hệ thống SOC cần được xử lý.

5. Báo cáo kết quả khắc phục, xử lý sự cố mất an toàn thông tin mạng do Trung tâm SOC tỉnh Yên Bái phát hiện.

Điều 11. Bảo trì, bảo dưỡng Trung tâm SOC tỉnh Yên Bái

1. Đơn vị vận hành có trách nhiệm thực hiện bảo trì, bảo dưỡng hệ thống theo quy trình và kế hoạch được phê duyệt.

2. Việc thực hiện bảo trì, bảo dưỡng các hệ thống do đơn vị vận hành thực hiện hoặc thuê dịch vụ.

3. Thời gian bảo trì, bảo dưỡng từng thiết bị, phần mềm thực hiện theo yêu cầu thực tiễn và khuyến nghị của nhà cung cấp. Bảo trì, bảo dưỡng tổng thể toàn bộ hệ thống ít nhất 01 lần trên 01 năm.

4. Việc thực hiện bảo trì, bảo dưỡng không được làm gián đoạn và ảnh hưởng đến tình hình hoạt động của Trung tâm SOC tỉnh Yên Bái; Quá trình bảo trì, bảo dưỡng phải thực hiện theo đúng kịch bản, quy trình và ghi nhật ký về tình trạng hoạt động trước và sau khi thực hiện.

Điều 12. Quy định đánh giá định kỳ Trung tâm SOC tỉnh Yên Bái

Các nội dung kiểm tra, đánh giá:

1. Tình hình sử dụng thiết bị, phần mềm của hệ thống SOC tỉnh Yên Bái.

2. Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về đảm bảo an toàn hệ thống SOC tỉnh Yên Bái theo cấp độ 3 đã được Ủy ban nhân dân tỉnh phê duyệt.

3. Kiểm tra, đánh giá hiệu quả của biện pháp đảm bảo an toàn thông tin theo thiết kế đã được phê duyệt tại Quyết định số 2232/QĐ-UBND ngày 31/10/2019.

4. Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống SOC tỉnh Yên Bái.

5. Kiểm tra, đánh giá tuân thủ các quy định tại Quy chế này.

Chương III
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC, CÁ NHÂN QUẢN LÝ, VẬN HÀNH TRUNG TÂM SOC TỈNH YÊN BÁI

Điều 13. Trách nhiệm cơ quan quản lý

1. Tham mưu Ủy ban nhân dân tỉnh nâng cấp và mở rộng Trung tâm SOC tỉnh Yên Bái đáp ứng yêu cầu đảm bảo an toàn thông tin phục vụ xây dựng chính quyền điện tử, phát triển đô thị thông minh và chuyển đổi số của tỉnh.

2. Phối hợp chặt chẽ với các cơ quan, đơn vị thực hiện việc quản lý tài sản đối với các thiết bị, phần mềm được cài đặt, vận hành tại các cơ quan, đơn vị trong tỉnh.

3. Ban hành các quy trình vận hành, bảo trì hệ thống SOC và quy trình giám sát, bảo vệ các hệ thống thông tin của tỉnh.

4. Tổng hợp kinh phí duy trì hoạt động, nâng cấp, mở rộng và phát triển Trung tâm SOC tỉnh Yên Bái và thẩm định kế hoạch bảo trì, bảo dưỡng định kỳ do đơn vị vận hành lập, trình cấp có thẩm quyền xem xét, quyết định.

Điều 14. Trách nhiệm của đơn vị vận hành

1. Bố trí cán bộ trực giám sát, điều hành hệ thống 24 giờ trong các ngày, 7 ngày trong các tuần.

2. Thực hiện điều hành xử lý các cảnh báo, phối hợp với đội ứng cứu sự cố an toàn thông tin mạng tỉnh và các đơn vị có liên quan kịp thời xử lý sự cố ngay sau khi phát hiện trên hệ thống.

3. Phải tổ chức thực hiện đầy đủ việc ghi nhật ký lập hồ sơ theo dõi quá trình phát hiện, phân tích và xử lý sự cố.

4. Hàng năm phải lập kế hoạch bảo trì, bảo dưỡng hệ thống trình cơ quan quản lý xem xét trình cấp có thẩm quyền phê duyệt. Thực hiện báo cáo theo điều 10 của Quy chế này.

5. Lập dự toán kinh phí duy trì hoạt động, nâng cấp, mở rộng và phát triển Trung tâm SOC báo cáo đơn vị quản lý để trình cấp có thẩm quyền xem xét, quyết định.

6. Hàng năm hoặc khi phát sinh yêu cầu mới tổ chức đào tạo, tập huấn cho thành viên của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh để nâng cao hiệu quả quản lý, vận hành Trung tâm SOC tỉnh Yên Bái.

Điều 15. Trách nhiệm của cán bộ vận hành

1. Tuân thủ theo các quy trình, quy định về quản lý, vận hành và xử lý sự cố tại Trung tâm SOC tỉnh Yên Bái.

2. Quản trị viên vận hành hệ thống truy cập, khai thác, sử dụng thông tin tại Trung tâm SOC tỉnh Yên Bái theo trách nhiệm và phân quyền được quy định; việc khai thác, sử dụng thông tin phải bảo đảm nguyên tắc bảo mật, không được tự ý cung cấp thông tin ra bên ngoài.

3. Bảo vệ bí mật thông tin tài khoản cá nhân, hoặc tài khoản của cơ quan, đơn vị khi được phân công nắm giữ, đồng thời phải thay đổi ngay mật khẩu tài khoản khi mới được cấp và tự chịu trách nhiệm trong việc quản lý, bảo vệ mật khẩu của tài khoản, không được cho người khác sử dụng tài khoản cá nhân hoặc của cơ quan, đơn vị. Trường hợp thay đổi nhân sự quản trị, vận hành Trung tâm SOC tỉnh, yêu cầu bắt buộc phải thay đổi mật khẩu để đảm bảo tính bảo mật của hệ thống.

4. Không đặt chế độ tự động ghi nhớ mật khẩu của các trình duyệt trong mọi trường hợp sử dụng đối với các phần mềm, ứng dụng trong cơ quan nhà nước.

5. Đặt mật khẩu đăng nhập, truy cập hệ thống thông tin có độ phức tạp cao (có độ dài tối thiểu 8 ký tự bao gồm: Ký tự thường, ký tự hoa, ký tự số và ký tự đặc biệt như: !, @, #, $, %); phải được thay đổi ít nhất 03 tháng một lần cho tất cả các tài khoản truy cập vào hệ thống máy chủ, thiết bị mạng, máy tính, các ứng dụng.

Điều 16. Trách nhiệm của các cơ quan, đơn vị có liên quan đến Trung tâm SOC tỉnh Yên Bái

1. Có trách nhiệm phối hợp với đơn vị vận hành Trung tâm SOC tỉnh Yên Bái thực hiện một số nội dung sau:

a) Bảo quản, duy trì hoạt động của hệ thống thiết bị, phần mềm đặt tại cơ quan, đơn vị, đảm bảo duy trì kết nối với Trung tâm SOC tỉnh Yên Bái. Khi phát hiện hệ thống bị lỗi, không hoạt động phải kịp thời thông báo về Trung tâm SOC tỉnh Yên Bái.

b) Phối hợp kịp thời xử lý các lỗi, lỗ hổng bảo mật, nguy cơ mất an toàn thông tin trên hệ thống thông tin của các cơ quan, đơn vị được phát hiện trên hệ thống SOC tỉnh Yên Bái.

c) Phối hợp kịp thời xử lý các sự cố an toàn thông tin khi có sự cố xảy ra.

2. Phải tuân thủ các quy định về an toàn bảo mật thông tin, quản lý vận hành và khai thác Trung tâm SOC tỉnh Yên Bái.

3. Trường hợp cơ quan, đơn vị phát hiện sự cố, phải kịp thời thông báo ngay cho đơn vị vận hành Trung tâm SOC tỉnh Yên Bái để phối hợp xử lý.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 17. Sở Thông tin và Truyền thông

1. Quản lý nhà nước về chuyên môn, nghiệp vụ với hoạt động của Trung tâm SOC tỉnh Yên Bái.

2. Thẩm định kỹ thuật với các nội dung nâng cấp, mở rộng và phát triển hoạt động của Trung tâm SOC tỉnh Yên Bái.

3. Điều phối các hoạt động đảm bảo an toàn thông tin trên địa bàn tỉnh, chủ trì duy trì hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng tỉnh trên cơ sở phối hợp với Trung tâm SOC tỉnh Yên Bái.

4. Đầu mối tiếp nhận Báo cáo của Trung tâm SOC tỉnh Yên Bái và các đơn vị có liên quan để tổng hợp báo cáo tình hình đảm bảo an toàn thông tin trên địa bàn tỉnh với Ủy ban nhân dân tỉnh, Bộ Thông tin và Truyền thông.

5. Sở Thông tin và Truyền thông tham mưu Ủy ban nhân dân tỉnh tỉnh giao đơn vị vận hành.

Điều 18. Sở Tài chính

Thẩm định kinh phí duy trì hoạt động, nâng cấp, mở rộng và phát triển của Trung tâm SOC tỉnh trình Ủy ban nhân dân tỉnh xem xét, quyết định.

Điều 19. Công an tỉnh

1. Kiểm tra, đánh giá điều kiện bảo đảm an ninh mạng đối với thiết bị phần cứng là thành phần của Trung tâm SOC Yên Bái.

2. Phối hợp với các cơ quan chức năng kiểm tra, đánh giá công tác bảo đảm an ninh mạng, an toàn thông tin đối với Trung tâm SOC Yên Bái.

Điều 20. Tổ chức thực hiện

1. Giao Sở Thông tin và Truyền thông chủ trì, phối hợp với các sở, ngành có liên quan tổ chức thực hiện quy chế này.

2. Trong quá trình thực hiện quy chế, nếu có khó khăn, vướng mắc, các cơ quan, đơn vị phản ánh bằng văn bản về Sở Thông tin và Truyền thông để tổng hợp báo cáo Ủy ban nhân dân tỉnh xem xét, sửa đổi, bổ sung cho phù hợp.

3. Các nội dung khác không có trong Quy chế này được thực hiện theo quy định của pháp luật hiện hành. Trường hợp có quy định khác của Trung ương điều chỉnh bổ sung thay thế các quy định, quy trình nội dung tại quy chế này thì thực hiện theo quy định mới./.