ỦY BAN NHÂN DÂN TỈNH BẾN TRE	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 33 /2023/QĐ-UBND	*Bến Tre, ngày 22 tháng 8 năm 2023*

QUYẾT ĐỊNH
Ban hành Quy chế Quản lý, khai thác và vận hành Trung tâm Giám sát An ninh mạng (SOC) tỉnh Bến Tre

ỦY BAN NHÂN DÂN TỈNH BẾN TRE

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 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 An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và đảm bảo an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Căn cứ Thông tư số 12/2019/TT-BTTTT ngày 05 tháng 11 năm 2019 của Bộ Thông tin và Truyền thông về việc sửa đổi, bổ sung một số điều của Thông tư số 27/2017/TT-BTTTT ngày 20 tháng 10 năm 2017 của Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 1675/TTr-STTTT ngày 18 tháng 8 năm 2023.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này là Quy chế Quản lý, khai thác và vận hành Trung tâm Giám sát An ninh mạng (SOC) tỉnh Bến Tre.

Điều 2. Điều khoản thi hành

1. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch Ủy ban nhân dân các

huyện, thành phố; Chủ tịch Ủy ban nhân dân các xã, phường, thị trấn và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này.

2. Quyết định này có hiệu lực thi hành kể từ ngày 04 tháng 9 năm 2023./.

Nơi nhận:
- Như Điều 2;
- Văn phòng Chính phủ;
- Bộ Thông tin và Truyền thông;
- Cục Kiểm tra văn bản QPPL - Bộ Tư pháp;
- TT.TU, TT.HĐND tỉnh;
- Chủ tịch, các PCT.UBND tỉnh;
- Đoàn ĐBQH tỉnh;
- Văn phòng Tỉnh ủy;
- UBMTTQ và các tổ chức CT-XH tỉnh;
- Các sở, ban, ngành tỉnh;
- Chánh, PCVP.UBND tỉnh;
- Sở Tư pháp;
- Báo ĐK, Đài PTTH, Cổng TTĐT;
- UBND các huyện, thành phố;
- UBND các xã, phường, thị trấn;
- Phòng: KGVX, TH;
- Lưu: VT, Ph.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Trần Ngọc Tam

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

QUY CHẾ
Quản lý, khai thác và vận hành Trung tâm Giám sát An ninh mạng (SOC) tỉnh Bến Tre

(Kèm theo Quyết định số 33 /2023/QĐ-UBND ngày 22 tháng 8 năm 2023 của Ủy ban nhân dân tỉnh Bến Tre)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định việc quản lý, khai thác và vận hành Trung tâm Giám sát An ninh mạng tỉnh Bến Tre (gọi tắt là Trung tâm SOC tỉnh).

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

Điều 2. Giải thích từ ngữ

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

1. Trung tâm SOC tỉnh (SOC - Security Operation Center): hệ thống công cụ phần cứng, phần mềm được cài đặt tại Trung tâm tích hợp dữ liệu tỉnh có kết nối tới Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC - National Cyber Security Center) 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.

2. Hệ thống thông tin: là một 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.

3. Sự cố an toàn thông tin: 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.

4. APT - Advanced Persistent Threat: tấn công có chủ đích.

5. IPS/IDS - Intrusion Prevention Systems/Intrusion Detection System: hệ thống phòng chống, phát hiện tấn công.

6. SIEM - Security Information and Event Management: thu thập, quản lý và phân tích sự kiện an ninh thông tin tập trung.

7. EDR - Endpoint Detection & Response: phòng, chống tấn công lớp đầu cuối.

8. SOAR - Security Orchestration, Automation and Response: điều phối, tự động hóa phản ứng an ninh thông tin tập trung.

9. NSM - Network Security Monitoring: giám sát cảnh báo trên lớp mạng.

Điều 3. Chủ sở hữu, quản lý, vận hành Trung tâm SOC tỉnh

1. Cơ quan chủ sở hữu Trung tâm SOC tỉnh *(gọi tắt là Cơ quan chủ quản)*: Ủy ban nhân dân tỉnh Bến Tre.

2. Cơ quan chịu trách nhiệm quản lý Trung tâm SOC tỉnh *(gọi tắt là Cơ quan quản lý)*: Sở Thông tin và Truyền thông.

3. Đơn vị vận hành, khai thác Trung tâm SOC tỉnh *(gọi tắt là Đơn vị vận hành)*: Trung tâm Công nghệ thông tin và Truyền thông Bến Tre.

Điều 4. Các chức năng và phân hệ của Trung tâm SOC tỉnh

1. Các chức năng của Trung tâm SOC tỉnh

a) Phòng, chống tấn công từ chối dịch vụ.

b) Tường lửa bảo vệ lớp mạng trong hệ thống.

c) Giám sát an toàn thông tin tập trung với đầy đủ các chức năng, hỗ trợ chia sẻ, kết nối với NCSC và các hệ thống giám sát, quản lý an toàn thông tin tập trung khác.

d) Bảo vệ hệ thống máy tính được giám sát trong hệ thống thông tin như Phát hiện và ngăn chặn các loại tấn công APT, 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.

đ) Giám sát tập trung các thiết bị đầu cuối đảm bảo an toàn, an ninh thông tin theo quy định.

2. Các phân hệ của Trung tâm SOC tỉnh

a) Phân hệ thu thập, quản lý và phân tích sự kiện an ninh thông tin tập trung (SIEM).

b) Phân hệ phòng, chống tấn công trên thiết bị đầu cuối (EDR).

c) Phân hệ điều phối, tự động hóa phản ứng an ninh thông tin tập trung (SOAR).

d) Phân hệ giám sát cảnh báo trên lớp mạng (NSM).

Điều 5. Nguyên tắc quản lý, khai thác và vận hành Trung tâm SOC tỉnh

1. Chủ động theo dõi, phân tích, phòng ngừa để kịp thời phát hiện, ngăn chặn, xử lý sự cố an toàn thông tin.

2. Khi phát hiện sự cố phải kịp thời thông báo đến cơ quan chịu trách nhiệm quản lý Trung tâm SOC tỉnh để thực hiện điều phối, ngăn chặn, xử lý.

3. Hệ thống phải vận hành hoạt động thường xuyên, liên tục, ổn định 24/7 các ngày trong tuần.

Chương II
QUẢN LÝ, KHAI THÁC VÀ VẬN HÀNH TRUNG TÂM SOC TỈNH

Điều 6. Quy định quản lý Trung tâm SOC tỉnh

1. Đối tượng quản lý tại Trung tâm SOC tỉnh

a) Trung tâm tích hợp dữ liệu tỉnh Bến Tre.

b) Hệ thống thông tin, phần mềm và cơ sở dữ liệu của các sở, ban, ngành tỉnh, Ủy ban nhân dân cấp huyện, Ủy ban nhân dân cấp xã.

c) Các thiết bị đầu cuối tại các cơ quan, đơn vị trên địa bàn tỉnh được thiết lập, kết nối về Trung tâm SOC tỉnh.

d) Hệ thống thông tin khác có liên quan.

2. Quy định quản lý hệ thống thông tin của Trung tâm SOC tỉnh

a) Việc giám sát phải được thực hiện liên tục 24/7 các ngày trong 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) 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.

c) Xử lý sự cố an toàn thông tin: phân tích các nhật ký hệ thống, 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.

3. Quản lý danh mục hồ sơ

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

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

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

d) Hồ sơ theo dõi xử lý sự cố.

đ) Bảng thống kê danh sách thiết bị, phần mềm tại Trung tâm SOC tỉnh; thiết bị, phần mềm lắp đặt và cài tại các cơ quan, đơn vị, địa phương; biên bản bàn giao thiết bị cho người quản trị, người sử dụng (nếu có).

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

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

h) Các hồ sơ, tài liệu kỹ thuật khác.

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

Điều 7. Quy định khai thác Trung tâm SOC tỉnh

1. Phân loại mức độ của các sự cố mất an toàn thông tin

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.

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 cơ quan, đơn vị.

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, đơn vị

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.

2. Quy trình xử lý sự cố mất an toàn 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 theo các nội dung sau:

a) Bước 1: Ghi nhận sự cố

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

Các sự cố được báo cáo về Cơ quan quản lý để điều phối xử lý sự cố và các cơ quan, đơn vị có liên quan biết phối hợp thực hiện.

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 sự cố

Phân tích sơ bộ về mức độ sự cố và phạm vi ảnh hưởng qua đó có thể phân loại mức độ sự cố. Đơn vị vận hành 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 Điều 7 Quy chế này.

c) Bước 3: Ngăn chặn

Đơn vị vận hành phối hợp với Tổ 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 kết nối mạng hoặc dịch vụ đang gặp sự cố.

d) Bước 4: Thu thập bằng chứng và truy tìm thủ phạm

Đơn vị vận hành chịu trách nhiệm thu thập các tệp tin dữ liệu có lưu 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.

đ) Bước 5: 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 phối hợp với Tổ ứng cứu sự cố an toàn thông tin mạng tỉnh để thực hiện loại bỏ nguyên nhân gây ra sự cố.

Nếu ngoài khả năng của Tổ ứng cứu thì Đơn vị vận hành phối hợp với Tổ ứng cứu và các cơ quan liên quan báo cáo Cơ quan chủ quản, Công an tỉnh và cơ quan chuyên trách về an toàn thông tin, Trung tâm ứng cứu an toàn không gian mạng thuộc Bộ Thông tin và Truyền thông để hỗ trợ điều phối ứng cứu.

e) Bước 6: Khôi phục

Sau khi đã loại bỏ nguyên nhân gây ra sự cố khỏi tất cả các hệ thống, Đơn vị vận hành phối hợp với Tổ 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.

g) Bước 7. Hoạt động sau sự cố

Đơn vị vận hành đánh giá, đề xuất các biện pháp 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 các cơ quan, đơn vị có liên quan kịp thời theo quy định cụ thể tại Điều 11 của Quy chế này.

3. Quy trình xử lý sự cố an toàn thông tin hệ thống giám sát tại Trung tâm SOC tỉnh

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 các nhật ký của hệ thống.

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

e) Khôi phục hệ thống sau sự cố.

4. Trao đổi, cung cấp, chia sẻ thông tin Trung tâm SOC tỉnh

a) Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia, thực hiện đăng ký đầy đủ các dãy 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.

b) Cung cấp định kỳ tình hình giám sát an toàn thông tin cho các cơ quan, đơn vị; phối hợp chặt chẽ với Tổ ứng cứu sự cố an toàn thông tin mạng tỉnh, 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 toàn, an ninh thông tin.

c) Kết nối, chia sẻ thông tin với Trung tâm Điều hành thông minh để phục vụ công tác theo dõi, chỉ đạo điều hành của lãnh đạo tỉnh.

d) Hình thức trao đổi thông tin

- Gọi điện thoại trực tiếp.

- Gửi thông báo qua hộp thư điện tử công vụ.

- Gửi thông báo bằng văn bản đến cơ quan, đơn vị.

Điều 8. Quy định về vận hành Trung tâm SOC tỉnh

1. Đơn vị vận hành có trách nhiệm lập kế hoạch bảo trì, bảo dưỡng và nâng cấp hệ thống hàng năm trình cơ quan có thẩm quyền phê duyệt.

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

3. Tối thiểu 01 năm một lần, Trung tâm SOC tỉnh lựa chọn đơn vị có năng lực về an toàn thông tin để thực hiện kiểm tra, đánh giá, rà quét, phát hiện lỗ hổng, điểm yếu, kiểm thử xâm nhập hệ thống để có giải pháp phòng ngừa, đảm bảo an toàn thông tin.

4. Kiểm tra đánh giá định kỳ Trung tâm SOC tỉnh

a) Tình hình sử dụng trang thiết bị công nghệ thông tin của Trung tâm SOC tỉnh.

b) Kiểm tra, đánh giá hiệu quả của giải pháp việc tuân thủ quy định của pháp luật về đảm bảo an toàn thông tin theo cấp độ đã được phê duyệt.

c) Kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập Trung tâm SOC tỉnh.

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

5. Bảo trì, bảo dưỡng, nâng cấp Trung tâm SOC tỉnh

a) Đơn vị vận hành có trách nhiệm lập kế hoạch bảo trì, bảo dưỡng và nâng cấp hệ thống hàng năm trình cơ quan có thẩm quyền phê duyệt.

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

c) Tối thiểu 01 năm một lần, Trung tâm SOC tỉnh lựa chọn đơn vị có năng lực về an toàn thông tin để thực hiện kiểm tra, đánh giá, rà quét, phát hiện lỗ hổng, điểm yếu, kiểm thử xâm nhập hệ thống để có giải pháp phòng ngừa, đảm bảo an toàn thông tin.

Điều 9. Quy định về báo cáo

a) Đơn vị vận hành phải có báo cáo định kỳ hàng tháng, hàng quý, hàng năm về kết quả giám sát, phát hiện, xử lý các cảnh báo và sự cố của Trung tâm SOC tỉnh cho bộ phận thường trực Tổ ứng cứu sự cố an toàn thông tin mạng tỉnh, Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao và các tổ chức có liên quan (nếu có).

b) Báo cáo đột xuất cho thường trực Tổ ứng cứu sự cố an toàn thông tin mạng tỉnh khi phát hiện sự cố mất an toàn thông tin.

c) 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 cần được xử lý.

d) Báo cáo kết quả khắc phục, xử lý sự cố mất an toàn thông tin mạng.

Chương III
TỔ CHỨC THỰC HIỆN

Điều 10. Trách nhiệm Sở Thông tin và Truyền thông

1. Tham mưu Ủy ban nhân dân tỉnh nâng cấp và mở rộng Trung tâm SOC tỉnh 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. Chủ trì, phối hợp với các cơ quan, đơn vị trên địa bàn tỉnh và các tổ chức có liên quan trong việc quản lý, khai thác và vận hành Trung tâm SOC tỉnh.

3. Hướng dẫn, hỗ trợ kỹ thuật, đào tạo, tập huấn kiến thức về an toàn thông tin cho các cơ quan, đơn vị trên địa bàn tỉnh.

4. Tuyên truyền, phổ biến cho các cơ quan, đơn vị các quy định của pháp luật về an toàn thông tin.

5. Bố trí nhân lực vận hành Trung tâm SOC tỉnh đảm bảo hoạt động 24/7 các ngày trong tuần.

6. Hàng năm, dự trù kinh phí đảm bảo hoạt động của Trung tâm SOC tỉnh gửi Sở Tài chính thẩm định trình Ủy ban nhân dân tỉnh phê duyệt.

Điều 11. Trách nhiệm Sở Tài chính

Chủ trì, phối hợp với Sở Thông tin và Truyền thông trình Ủy ban nhân dân tỉnh xem xét, phê duyệt kinh phí để đảm bảo hoạt động của Trung tâm SOC tỉnh.

Điều 12. Trách nhiệm Công an tỉnh

1. Phối hợp với Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao - Bộ Công an (A05) kiểm tra, đánh giá điều kiện bảo đảm an toàn, an ninh thông tin đối với trang thiết bị công nghệ thông tin tại Trung tâm SOC tỉnh.

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

Điều 13. Trách nhiệm của cán bộ, công chức, viên chức các Sở, Ban, ngành và địa phương tham gia vận hành Trung tâm SOC tỉnh

Có trách nhiệm phối hợp với Đơn vị vận hành thực hiện một số nội dung sau:

a) Bảo đảm hệ thống thông tin đặt tại cơ quan, đơn vị luôn kết nối với Trung tâm SOC tỉnh.

b) Khi phát hiện hệ thống bị lỗi, không hoạt động phải kịp thời thông báo về Trung tâm SOC tỉnh để phối hợp xử lý các lỗi, lỗ hổng bảo mật, nguy cơ mất an toàn thông tin trên hệ thống thông tin.

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

Điều 14. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chịu trách nhiệm tuyên truyền, phổ biến, hướng dẫn, tổ chức triển khai và kiểm tra thực hiện Quy chế này.

2. Thủ trưởng các cơ quan, đơn vị trên địa bàn tỉnh và các tổ chức, cá nhân có liên quan trong phạm vi chức năng, nhiệm vụ của mình, có trách nhiệm tổ chức triển khai thực hiện nghiêm túc Quy chế này.

3. Những nội dung khác liên quan đến hoạt động quản lý, khai thác và vận hành Trung tâm SOC tỉnh không quy định tại Quy chế này được thực hiện theo quy định của pháp luật hiện hành.

4. Trong quá trình triển khai thực hiện, nếu phát sinh vướng mắc, bất cập, các cơ quan, tổ chức, cá nhân phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân tỉnh xem xét, sửa đổi, bổ sung Quy chế cho phù hợp./.