ỦY BAN NHÂN DÂN TỈNH QUẢNG NGÃI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập- Tự do- Hạnh phúc
Số: 365/QĐ-UBND	*Quảng Ngãi, ngày 22 tháng 3 năm 2023*

QUYẾT ĐỊNH
Ban hành Quy chế vận hành Hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung (SOC) tỉnh Quảng Ngãi

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH QUẢNG NGÃI

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19 tháng 6 năm 2015; 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 Giao dịch điện tử ngày 29 tháng 11 năm 2005;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

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

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 Chỉ thị số 14/CT-TTg ngày 07 tháng 6 năm 2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Thông tư số 39/2017/TT-BTTTT ngày 15 tháng 12 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông về việc ban hành Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước;

Theo đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 292/TTr-STTTT ngày 06 tháng 3 năm 2023.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế vận hành Hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung (SOC) tỉnh Quảng Ngãi.

Điều 2. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh, Giám đốc Công an tỉnh, Giám đốc Sở Thông tin và Truyền thông; Thủ trưởng các sở, ban, ngành, hội, đoàn thể tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố và các cơ quan, tổ chức và cá nhân khác có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ Thông tin và Truyền thông;
- Thường trực Tỉnh ủy;
- Thường trực HĐND tỉnh;
- CT, các PCT UBND tỉnh;
- Đoàn Đại biểu Quốc hội tỉnh;
- Ban Thường trực UBMTTQVN tỉnh;
- Viettel Chi nhánh Quảng Ngãi;
- Báo Quảng Ngãi; Đài PT – TH tỉnh;
- VPUB: PCVP, TTPVKSTTHC, CBTH
- Lưu: VT, KGVXn202

CHỦ TỊCH

Đặng Văn Minh

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

QUY CHẾ
Vận hành Hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung tỉnh Quảng Ngãi

(Ban hành kèm theo Quyết định số 365/QĐ-UBND ngày 22/3/2023 của Chủ tịch UBND tỉnh)

Chương I
QUY ĐỊNH CHUNG

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

1. Phạm vi điều chỉnh: Quy chế này quy định về vận hành và khai thác sử dụng Hệ thống giám sát, điều hành an toàn, an ninh mạng tập trung tỉnh Quảng Ngãi *(sau đây gọi tắt là Hệ thống SOC).*

2. Đối tượng áp dụng: Quy chế này được áp dụng đối với các đơn vị và cá nhân liên quan đến việc tham gia quản lý, sử dụng và vận hành Hệ thống SOC.

Điều 2. Giải thích từ ngữ

1. An toàn, an ninh thông tin bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin trước các nguy cơ tự nhiên hoặc do con người gây ra. An toàn, an ninh thông tin bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng.

2. Hệ thống SOC là hệ thống rà soát, phân tích, báo cáo và ngăn chặn các mối đe dọa an ninh mạng, đồng thời ứng phó với bất kỳ sự cố nào xảy ra với máy tính, máy chủ và hệ thống mạng mà Hệ thống SOC giám sát.

Chương II
GIÁM SÁT, ĐIỀU HÀNH AN TOÀN, AN NINH MẠNG TẬP TRUNG TỈNH QUẢNG NGÃI

Điều 4. Nguyên tắc giám sát

1. Đảm bảo được thực hiện thường xuyên, liên tục.

2. Chủ động theo dõi, phân tích, phòng ngừa để kịp thời phát hiện, ngăn chặn rủi ro, sự cố an toàn thông tin.

3. Đảm bảo hoạt động ổn định, bí mật cho thông tin được cung cấp, trao đổi trong quá trình giám sát.

4. Có sự điều phối, kết hợp chặt chẽ, hiệu quả giữa hoạt động giám sát của các đơn vị và cá nhân liên quan.

Điều 5. Kiểm soát truy nhập và xác thực

1. Cấp phát quyền truy cập, sử dụng và khai thác hệ thống phải bảo đảm chặt chẽ, bảo đảm đúng mục đích sử dụng.

2. Vô hiệu hóa hoặc xóa các tài khoản đã được đăng ký trên hệ thống nhưng không làm việc trong hệ thống.

3. Tránh nguy cơ bị tấn công brute force password với các username mặc định như: administrator, guest,...

4. Đặt mật khẩu phức tạp cho tài khoản; mật khẩu tài khoản hệ thống phải được thay đổi trong thời gian 60 ngày.

5. Giới hạn số lần đăng nhập không thành công vào hệ thống là 05 lần. Sau 05 lần đăng nhập không thành công, tài khoản sẽ bị khóa trong thời gian ít nhất là 05 phút hoặc yêu cầu xác thực.

6. Phát hiện và xử lý kịp thời những trường hợp người dùng truy nhập bất hợp pháp hoặc thao tác vượt quá giới hạn cho phép.

Điều 6. Quy định lưu trữ log

1. Thu thập đầy đủ nhật ký (log file) phản ánh hoạt động của các ứng dụng, hệ thống thông tin, thiết bị an toàn thông tin.

2. Thời gian lưu trữ log hệ thống tối thiểu là 03 tháng (Theo TCVN 11930:2017 quy định về thời gian lưu trữ log của hệ thống thông tin cấp độ 3).

Điều 7. Quy định về phối hợp xử lý

1. Các đầu mối giám sát trao đổi, cung cấp thông tin cho nhau nhằm mục đích phối hợp trong công tác giám sát, cảnh báo, ứng cứu sự cố và tăng tính chủ động ứng phó với các nguy cơ, mối đe dọa, phương thức, thủ đoạn tấn công an toàn thông tin của tổ chức, cá nhân.

2. Nguyên tắc phối hợp:

a) Các thông tin trao đổi, phối hợp phải kịp thời, chính xác và áp dụng các biện pháp quản lý, kỹ thuật phù hợp để bảo mật thông tin trao đổi.

b) Chủ động xác minh thông tin trao đổi nhằm đảm bảo tính xác thực của thông tin.

Điều 8. Quy trình phối hợp xử lý sự cố

1. Khi phát hiện xảy ra sự cố, đơn vị sử dụng báo cáo sự cố cho Sở Thông tin và Truyền thông, đồng thời thông báo cho đơn vị cho thuê dịch vụ.

2. Sau khi tiếp nhận sự cố, đơn vị cho thuê dịch vụ tổ chức ngay việc kiểm tra và có biện pháp xử lý sự cố kịp thời nhằm đảm bảo hệ thống hoạt động an toàn, liên tục và khắc phục trong vòng 24 giờ đối với sự cố nghiêm trọng, 72 giờ đối với sự cố bình thường.

3. Sau khi hoàn thành việc xử lý sự cố, trong vòng 04 giờ đơn vị cho thuê dịch vụ phải có báo cáo về việc xử lý sự cố cho Sở Thông tin và Truyền thông và đơn vị sử dụng có liên quan.

Chương III
QUY ĐỊNH TRÁCH NHIỆM CỦA CÁC CƠ QUAN, TỔ CHỨC, CÁ NHÂN TRONG VIỆC QUẢN LÝ, SỬ DỤNG VÀ VẬN HÀNH HỆ THỐNG SOC

Điều 9. Trách nhiệm của đơn vị chủ quản (Sở Thông tin và Truyền thông)

1. Chủ trì, phối hợp với các đơn vị sử dụng xây dựng kế hoạch đầu tư, đề xuất kinh phí nâng cấp phần mềm đáp ứng nhu cầu vận hành của Hệ thống SOC để đảm bảo hệ thống được hoạt động thông suốt và ổn định.

2. Phối hợp với đơn vị cho thuê dịch vụ trong việc tổng hợp ý kiến đóng góp từ người dùng để xem xét sửa đổi, nâng cấp phần mềm nhằm cải tiến phần mềm ngày càng hoàn thiện và thân thiện với người sử dụng, đáp ứng tốt hơn trong việc sử dụng thực tế.

3. Chủ trì, phối hợp với đơn vị cho thuê dịch vụ thông báo bằng văn bản cho các cơ quan, đơn vị về việc xảy ra sự cố hoặc nguy cơ xảy ra sự cố có ảnh hưởng xấu đến việc quản lý và khai thác sử dụng phần mềm, đồng thời có các giải pháp khắc phục sự cố nếu có.

Điều 10. Trách nhiệm của đơn vị cho thuê dịch vụ

1. Cấu hình kết nối chia sẻ thông tin với Trung tâm Giám sát an toàn không gian mạng quốc gia (NCSC).

2. Thực hiện cài đặt, kiểm tra cấu hình các Agent (SE Agent, EDR Agent) tại các đơn vị sử dụng theo yêu cầu của đơn vị chủ quản.

3. Phối hợp với đơn vị vận hành thực hiện cấu hình các thiết bị mạng, bảo mật và các hệ thống liên quan để thu thập log, traffic phục vụ phân tích, giám sát.

4. Bảo mật thông tin, dữ liệu được thu thập từ Trung tâm dữ liệu tỉnh Quảng Ngãi và các hệ thống thông tin được kết nối giám sát trên Hệ thống SOC.

5. Đảm bảo duy trì hoạt động của hệ thống liên tục, thông suốt 24/7 trong thời gian sử dụng dịch vụ. Xử lý những sự cố kỹ thuật liên quan đến phần mềm cung cấp và các vấn đề phát sinh khi cung cấp dịch vụ và đảm bảo chất lượng dịch vụ trong quá trình khai thác sử dụng.

6. Cung cấp các thiết lập kỹ thuật, các liên kết, các hàm API có liên quan đến phần mềm của Hệ thống SOC trong phạm vi dịch vụ cung cấp theo yêu cầu của đơn vị chủ quản khi cần.

7. Báo cáo định kỳ hàng tuần, hàng tháng, năm và đột xuất tình hình sử dụng dịch vụ cho đơn vị chủ quản.

8. Thực hiện các nhiệm vụ khác thuộc trách nhiệm của bộ phận Phân tích cảnh báo (Tier 1) và bộ phận Ứng cứu, xử lý sự cố (Tier 3) theo hướng dẫn tại Công văn số 235/CATTT-ATHTTT ngày 08/4/2020 của Cục An toàn thông tin - Bộ Thông tin và Truyền thông.

Điều 11. Trách nhiệm của đơn vị vận hành *(Trung tâm Công nghệ thông tin và Truyền thông Quảng Ngãi - đơn vị trực thuộc Sở Thông tin và Truyền thông Quảng Ngãi)*

1. Được sử dụng tài khoản đặc quyền để thực hiện việc cập nhật, quản lý và khai thác phần mềm.

2. Theo dõi, phát hiện và báo cáo với cấp có thẩm quyền xem xét, xử lý các vấn đề phát sinh trong công tác quản lý phần mềm; đề xuất các biện pháp bảo đảm sử dụng và khai thác có hiệu quả phần mềm để cung cấp kịp thời, nhanh chóng, chính xác phục vụ yêu cầu quản lý và công tác chuyên môn; định kỳ hoặc đột xuất tổng hợp báo cáo đơn vị chủ quản.

3. Triển khai và áp dụng các biện pháp bảo đảm an toàn và bảo mật phần mềm, đảm bảo an toàn cơ sở dữ liệu của đơn vị.

4. Phối hợp đơn vị cho thuê dịch vụ thực hiện việc giám sát, đánh giá, báo cáo đơn vị chủ quản các rủi ro mất an toàn thông tin 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, an ninh thông tin.

5. Thực hiện nhiệm vụ của bộ phận Tiếp nhận và sử lý sự cố (Tier 2): Tiếp nhận sự cố từ Tier 1 thông qua email *(tùy theo mức độ sự cố, sự cần thiết)*; thực hiện cấu hình thiết lập các chính sách trên hệ thống *(hệ điều hành, thiết bị mạng/bảo mật, máy chủ web - web server, cơ sở dữ liệu)*; đánh giá, phân tích xử lý sự cố/ticket theo hướng dẫn định nghĩa trước. Kiểm tra và vá lỗ hổng, chặn các mã độc, cài/kiểm tra, quét virus; xác minh (verify) một số nghiệp vụ *(phát sinh tài khoản, thay đổi file/thư mục, mở cổng)*; khắc phục các lỗ hổng, điểm yếu khi được bên cung cấp dịch vụ cảnh báo. Phối hợp với đơn vị cho thuê dịch vụ đăng nhập hệ thống, điều tra, ứng cứu và xử lý sự cố. Phân tích gỡ mã độc, đối với các ticket *(không xử lý thành công hoặc sự cố nghiêm trọng)* thực hiện tạo sub tickets cho Tier 3 để đơn vị cho thuê dịch vụ xử lý.

6. Tổ chức đào tạo, bồi dưỡng để nâng cao trình độ chuyên môn, nghiệp vụ cho cán bộ tham gia vận hành Hệ thống SOC.

Điều 12. Trách nhiệm của đơn vị sử dụng ***(các cơ quan, đơn vị vận hành hệ thống thông tin đã được phê duyệt và thực hiện cài đặt, kết nối vào Hệ thống SOC)***

1. Bố trí 01 máy chủ phục vụ cài đặt phần mềm Network Security Monitoring (NSM) phát hiện và chống tấn công APT lớp mạng người dùng; mở kết nối các máy chủ cần bảo vệ về Trung tâm dữ liệu tỉnh bằng đường truyền riêng để bảo đảm về an toàn thông tin đối với các hệ thống liên quan.

2. Cung cấp thông tin chính xác về các máy chủ, máy trạm có nhu cầu cài đặt phần mềm giám sát bất thường SE Agent, EDR Agent.

3. Khi có thay đổi, bổ sung cũng như cài đặt lại hệ điều hành kịp thời thông báo lại cho đơn vị chủ quản để tiến hành phối hợp cài đặt bổ sung.

4. Không tự ý gỡ cài đặt các phần mềm có liên quan ra khỏi máy chủ, máy trạm khi chưa thông báo cho đơn vị chủ quản.

5. Phối hợp thực hiện việc giám sát, đánh giá, báo cáo Thủ trưởng cơ quan, đơn vị các rủi ro mất an toàn thông tin và mức độ nghiêm trọng của các rủi ro đó. Phối hợp với đơn vị chủ quản, đơn vị vận hành, đơn vị cho thuê dịch vụ và các đơn vị có liên quan trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn, an ninh thông tin.

6. Kiến nghị và đề xuất với cơ quan có thẩm quyền sửa đổi, bổ sung những quy định liên quan đến việc cập nhật, quản lý và khai thác phần mềm.

Điều 13. Trách nhiệm của các cơ quan, đơn vị có hệ thống thông tin trên Trung tâm dữ liệu tỉnh được cài đặt, kết nối vào Hệ thống SOC

1. Cử cán bộ phối hợp đơn vị vận hành trong quá trình cài đặt phần mềm giám sát bất thường SE Agent, EDR Agent trên máy chủ của đơn vị.

2. Không tự ý gỡ cài đặt các phần mềm giám sát bất thường SE Agent, EDR Agent ra khỏi máy chủ vận hành các hệ thống thông tin khi chưa thông báo cho Đơn vị vận hành.

3. Khi có thông báo về các rủi ro an toàn thông tin do Hệ thống SOC cảnh báo từ đơn vị vận hành, đơn vị chủ quản phải cử cán bộ phối hợp để kiểm tra, kịp thời phát hiện và khắc phục các sự cố an toàn, an ninh thông tin của hệ thống thông tin của đơn vị.

Chương IV
TỔ CHỨC THỰC HIỆN

Điều 14. Xử lý vi phạm

Tổ chức, cá nhân tham gia sử dụng, vận hành, quản lý Hệ thống SOC có hành vi vi phạm Quy chế này, tùy theo tính chất, mức độ vi phạm sẽ bị xử lý, kỷ luật theo quy định của pháp luật.

Điều 15. Điều khoản thi hành

1. Các đơn vị có trách nhiệm tổ chức triển khai, thực hiện nghiêm túc Quy chế này.

2. Sở Thông tin và Truyền thông có trách nhiệm hướng dẫn, kiểm tra, đôn đốc các sở, ban, ngành liên quan và các đơn vị trực thuộc triển khai thực hiện Quy chế này; định kỳ tổng hợp, báo cáo kết quả triển khai thực hiện theo quy định.

Trong quá trình thực hiện, nếu có những vấn đề phát sinh cần điều chỉnh, bổ sung, các cơ quan, đơn vị, kịp thời phản ánh về UBND tỉnh *(thông qua Sở Thông tin và Truyền thông)* để tổng hợp báo cáo UBND tỉnh xem xét, quyết định./.