UBND TỈNH KHÁNH HÒA
SỞ CÔNG THƯƠNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Số: 39 /KH-SCT

Khánh Hòa, ngày 22 tháng 5 năm 2025

KẾ HOẠCH

Ứng phó sự cố, bảo đảm an toàn thông tin mạng trong hoạt động của Sở Công Thương Khánh Hòa năm 2025

Triển khai thực hiện Kế hoạch số 5479/KH-UBND ngày 08/05/2025 của UBND tỉnh Khánh Hòa về Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2025; Sở Công Thương xây dựng Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2025 tại cơ quan như sau:

I. MỤC ĐÍCH

1. Củng cố nền tảng hạ tầng an toàn thông tin mạng, thích ứng chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin đối với các hệ thống thông tin thuộc phạm vi quản lý, sử dụng.

2. Tạo chuyển biến nhận thức đối với lực lượng công chức, viên chức và người lao động trong việc bảo đảm an toàn thông tin mạng khi truy cập, khai thác các hệ thông tin dùng chung, trọng yếu do UBND tỉnh triển khai.

II. YÊU CẦU

1. Tuyên truyền, tạo chuyển biến nhận thức phải ưu tiên hướng đến lãnh đạo các đơn vị hoặc cá nhân được giao phụ trách triển khai nhiệm vụ khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số.

2. Đầu tư xây dựng, nâng cấp hạ tầng an toàn thông tin mạng phải đáp ứng yêu cầu nhiệm vụ khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số, phù hợp phương án bảo đảm an toàn thông tin theo cấp độ được phê duyệt.

3. Tổ chức đánh giá các nguy cơ, sự cố an toàn thông tin mạng phải toàn diện, bao gồm tất cả các hệ thống thông tin thuộc phạm vi quản lý, sử dụng, so sánh và đối chiếu với phương án bảo đảm an toàn thông tin theo cấp độ được phê duyệt, triển khai để có kết luận chính xác và khách quan.

4. Phương án đối phó, ứng cứu, xử lý sự cố phải đánh giá đúng mức độ ngiêm trọng của sự cố xảy ra, có tính khả thi trong tình huống bất ngờ, khác kịch bản đã xây dựng.

III.NỘI DUNG THỰC HIỆN

1. Các nhiệm vụ cần triển khai trước khi sự cố xảy ra.

a. Tuyên truyền, phổ biến, nâng cao nhận thức:

- Nội dung trọng tâm: Luật An toàn thông tin mạng và các quy định, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng.

- Cách thức thực hiện: lồng ghép trong các văn bản chỉ đạo, điều hành, đăng tải trên Trang thông tin điện tử Sở Công Thương.

- Thời gian thực hiện: thường xuyên trong năm.

b. Tham gia chương trình đào tạo, bồi dưỡng kỹ năng đánh giá, ứng cứu khẩn cấp sự cố do Công an tỉnh và các đơn vị liên quan tổ chức.

- Phương thức thực hiện*:* thành viên Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tham dự.

- Thời gian thực hiện: trong năm 2025.

c. Phòng ngừa, giám sát, phát hiện sớm sự cố bằng cách kết nối với hệ thống Trung tâm Giám sát an toàn thông tin mạng (SOC) của tỉnh nhằm kiểm tra, đánh giá, rà quét, bóc gỡ, phân tích, xử lý mã độc; cảnh báo sự cố, rủi ro an toàn thông tin mạng, phần mềm độc hại đến các đơn vị thuộc, trực thuộc ngay khi nhận được thông tin từ Công an tỉnh và các đơn vị liên quan; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin cho các hệ thống thông tin thuộc phạm vi quản lý, vận hành theo hồ sơ đề xuất cấp độ được phê duyệt.

Rà soát, đánh giá tình hình triển khai phương án bảo đảm an toàn thông tin đối với hệ thống thông tin đã được phê duyệt hồ sơ đề xuất cấp độ, khắc phục điểm yếu tồn tại theo kết quả kiểm tra của Công an tỉnh thời gian vừa qua. Tiếp tục xây dựng, phê duyệt hồ sơ đề xuất cấp độ an toàn thông tin đối với Trang thông tin điện tử, Sàn Giao dịch Thương mại điện tử Khánh Hòa và các hệ thống thông tin được phát sinh trong quá trình thực hiện nhiệm vụ khoa học công nghệ, đổi mới sáng tạo và chuyển đổi số.

- Phương thức thực hiện*:* tự thực hiện, đồng thời phối hợp với Công an tỉnh và các đơn vị cung cấp dịch vụ liên quan.

- Thời gian thực hiện: thường xuyên trong năm.

d. Gia hạn phần mềm phòng chống mã độc bản quyền trên tất cả máy trạm, hạn chế tối đa việc sử dụng phần mềm bản crack trong hoạt động công vụ có khả năng gây ảnh hưởng nghiêm trọng đến an toàn thông tin mạng. Nghiên cứu đầu tư mua sắm thiết bị Firewall chuyên dùng để quản lý các vùng mạng nội bộ theo yêu cầu của Công an tỉnh.

- Phương thức thực hiện*:* tự thực hiện.

- Thời gian thực hiện: thường xuyên trong năm.

e. Tổ chức đánh giá các nguy cơ sự cố an toàn thông tin mạng

- Nội dung thực hiện:

+ Đánh giá tình hình quản lý, vận hành các hệ thống thông tin thuộc phạm vi quản lý thời gian vừa qua, thống kê đầy đủ sự cố an toàn thông tin mạng đã xảy ra và mức độ, phạm vi ảnh hưởng.

+ Đánh giá tình hình khắc phục sự cố an toàn thông tin mạng đã xảy ra thời gian vừa qua, phân tích rõ nguyên nhân xảy ra sự cố có liên quan đến phương án quản lý hay phương án kỹ thuật đã triển khai theo hồ sơ đề xuất cấp độ được phê duyệt.

+ Đánh giá phương án kỹ thuật đã triển khai liên quan sự cố xảy ra, dự báo nguy cơ sự cố có thể xảy ra thời gian tới dựa trên cấu hình trang thiết bị đã xảy ra sự cố.

+ Đánh giá phương án quản lý đã ban hành liên quan sự cố xảy ra, dự báo nguy cơ sự cố có thể xảy ra thời gian tới dựa trên điểm yếu, thiếu sót, hạn chế trong quy chế/quy định an toàn thông tin mạng đã ban hành.

- Phương thức thực hiện*:* tự thực hiện hoặc thuê đơn vị cung cấp dịch vụ an toàn thông tin mạng.

- Thời gian thực hiện: định kỳ 06 tháng (*trước ngày 10 tháng 06*), 01 năm (*trước ngày 05 tháng 12*).

f. Xây dựng phương án đối phó, ứng cứu đối với tình huống sự cố mất an toàn thông tin mạng thường gặp:

Nội dung thực hiện: các đơn vị quản lý, vận hành các hệ thống thông tin, chương trình ứng dụng trên môi trường mạng phải xây dựng tình huống, kịch bản sự cố an toàn thông tin mạng có thể xảy ra, ảnh hưởng đến hoạt động của hệ thống và đưa ra phương án đối phó, ứng cứu, ví dụ cụ thể như sau:

Tình huống sự cố mất an toàn thông tin mạng thường gặp đối với các máy trạm trong hệ thống mạng LAN là bị mã độc tấn công

– Tiêu chí để xác định đúng tính chất, mức độ nghiêm trọng của sự cố:

➢ Dịch vụ, tiện ích của hệ điều hành không hoạt động theo yêu cầu của người sử dụng.

➢ Xuất hiện nhiều tập tin lạ.

➢ Hệ điều hành tự động shutdown/restart/logoff hoặc tự động thay đổi thông tin, cấu hình ban đầu được mặc định mà không có sự can thiệp của người quản trị, vận hành hệ thống.

➢ Giao diện hệ điều hành tự động thay đổi mà không có sự điều chỉnh của người sử dụng.

➢ Dữ liệu người sử dụng bị mất hoặc thay đổi, không còn nguyên vẹn.

➢ Các hiện tượng trên xuất hiện thường xuyên, liên tục, cùng lúc tại nhiều máy trạm trên hệ thống, có khả năng gây tê liệt hoạt động công vụ trên môi trường mạng.

– Nguyên nhân, nguồn gốc sự cố:

➢ Người sử dụng truy cập website có tiềm ẩn nguy cơ, khả năng tấn công từ chối dịch vụ/tấn công sử dụng mã độc/tấn công truy cập trái phép, chiếm quyền điều khiển/tấn công thay đổi giao diện/tấn công phá hoại thông tin, dữ liệu, phần mềm,…

➢ Hệ điều hành máy trạm không có bản quyền dẫn đến hệ thống bảo mật không đủ mạnh để phòng chống sự xâm nhập của tin tặc từ môi trường mạng.

➢ Phần mềm phòng chống mã độc không có bản quyền hoặc chưa được cấu hình đầy đủ chức năng để chống lại mã độc trong quá trình truy cập mạng.

– Phương án đối phó, ứng cứu, khắc phục sự cố:

➢ Ngắt kết nối mạng các máy trạm bị sự cố, bật tường lửa của hệ điều hành, sử dụng phần mềm phòng, chống mã độc hiện có để quét toàn bộ hệ thống ổ đĩa nhằm phát hiện và tiêu diệt mã độc, ngăn chặn sự tấn công và thu hẹp phạm vi ảnh hưởng của sự cố.

➢ Xóa lịch sử các trình duyệt Web được sử dụng, gỡ bỏ các phần mềm bản crack ra khỏi hệ điều hành, nếu tình trạng sự cố không cải thiện, cài đặt hệ điều hành và phần mềm phòng chống mã độc có bản quyền cho máy trạm.

– Phương thức thực hiện: các đơn vị chuyên môn, trực thuộc phụ trách hệ thống thông tin tự xây dựng phương án, kịch bản hoặc phối hợp đơn vị cung cấp dịch vụ xây dựng phương án theo hướng dẫn của các cơ quan chuyên môn cấp trên.

– Thời gian thực hiện: sau khi Kế hoạch này được ban hành.

2. Quy trình ứng cứu, xử lý khẩn cấp sự cố khi có tấn công mạng xảy ra.

Theo Phụ lục 1 Kế hoạch này

IV. TỔ CHỨC THỰC HIỆN

Văn phòng Sở chủ trì, phối hợp với các phòng, đơn vị thuộc và trực thuộc Sở; tổ chức và cá nhân liên quan thực hiện Kế hoạch này.

Trên đây là Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng trong hoạt động của Sở Công Thương tỉnh Khánh Hòa năm 2025./.

Nơi nhận (VBĐT):
- Các phòng, đơn vị thuộc Sở;
- Trung tâm KC&XTTM;
- Chi cục QLTT;
- Công an tỉnh;
- Lưu: VT, VP, HN.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ CÔNG THƯƠNG
TỈNH KHÁNH HÒA

Huỳnh Tấn Hải

PHỤ LỤC 1

QUY TRÌNH ỨNG CỨU, XỬ LÝ KHẨN CẤP SỰ CỐ TẤN CÔNG MẠNG

(ban hành kèm theo Kế hoạch số: 39 /KH-SCT ngày 22 /5/2025 của Sở Công Thương)

STT	Quy trình	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp
I	**Phát hiện, tiếp nhận và thông báo, báo cáo sự cố**			
1	Phát hiện, tiếp nhận	Ghi nhận, tiếp nhận, tập hợp thông tin liên quan và tiến hành phân tích, xác minh, đánh giá sơ bộ tình hình và phân loại sự cố	Văn phòng Sở, các đơn vị chuyên môn, trực thuộc quản lý, vận hành hệ thống thông tin	Công an tỉnh; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (UCKCSC); Đơn vị cung cấp dịch vụ an toàn thông tin mạng
2	Thông báo**,** báo cáo sự cố	Phản hồi cho tổ chức, cá nhân gửi thông báo sự cố. Nếu thấy cần thiết, báo cáo tình hình ban đầu đến Công an tỉnh và Đội UCKCSC bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện hoặc thông qua hệ thống báo cáo, cảnh báo sự cố trên địa bàn tỉnh (*theo mẫu tại Phụ lục 2*)	Văn phòng Sở, các đơn vị chuyên môn, trực thuộc quản lý, vận hành hệ thống thông tin	Công an tỉnh; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (UCKCSC); Đơn vị cung cấp dịch vụ an toàn thông tin mạng
II	**Ứng cứu, khắc phục, xử lý sự cố**			
1	Ứng cứu ban đầu	- Ngắt kết nối mạng đối với máy chủ/máy trạm/thiết bị lưu trữ dữ liệu chuyên dụng và		

STT	Quy trình	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp
		tạm dừng các ứng dụng dịch vụ quan trọng trong hệ thống mạng (*nếu thấy cần thiết*). - Đánh giá ban đầu về sự cố sau khi ngắt kết nối mạng: do lỗi nguồn điện/đường truyền Internet/lỗi phần mềm ứng dụng/do thảm họa tự nhiên: cháy nổ, mưa bão, lũ lụt… hoặc do bị tấn công mạng.	Văn phòng Sở, các đơn vị chuyên môn, trực thuộc quản lý, vận hành hệ thống thông tin	Công an tỉnh; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (UCKCSC); Đơn vị cung cấp dịch vụ an toàn thông tin mạng
2	Xác định nguyên nhân sự cố	Xác định nguyên nhân sự cố dựa trên 03 tình huống: - Tình huống sự cố do bị tấn công mạng (từ chối dịch vụ, mã độc, chiếm quyền điều khiển, thay đổi giao diện, mã hóa phần mềm,…). - Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống (cập nhật, thay đổi cấu hình phần cứng, phần mềm, chính sách và thủ tục, trách nhiệm được quy định,…). - Tình huống sự cố do lỗi của người dùng cuối (chia sẻ, làm lộ, mất thông tin, thực hiện sai quy trình, quy chế, chính sách, thủ tục ATTT đã ban hành,…).	Văn phòng Sở, các đơn vị chuyên môn, trực thuộc quản lý, vận hành hệ thống thông tin	Công an tỉnh; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (UCKCSC); Đơn vị cung cấp dịch vụ an toàn thông tin mạng

STT	Quy trình	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp
3	Triển khai xử lý, khắc phục sự cố	- Xác định đối tượng, mục tiêu cần ưu tiên ứng cứu (*theo thứ tự mức độ quan trọng liên quan đến thành phần chức năng, ứng dụng dịch vụ, dữ liệu quan trọng cần bảo vệ, khôi phục*), tiến hành triển khai phương án đối phó, ứng cứu đối với tình huống sự cố mất an toàn thông tin mạng đã được xây dựng. - Tiêu diệt các mã độc, phần mềm độc hại trên toàn bộ máy chủ/máy trạm trong hệ thống; bổ sung các thiết bị phần cứng, phần mềm bảo đảm an toàn thông tin cho hệ thống; cấu hình lại các thông số an toàn cho hệ thống. - Trường hợp sự cố nghiêm trọng không tự xử lý được, báo cáo diễn biến tình hình đến Công an tỉnh và Đội UCKCSC để phối hợp xử lý.	Văn phòng Sở, các đơn vị chuyên môn, trực thuộc quản lý, vận hành hệ thống thông tin	Công an tỉnh; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (UCKCSC); Đơn vị cung cấp dịch vụ an toàn thông tin mạng
4	Khôi phục hệ thống	- Khôi phục một số kết nối cần thiết để hệ thống hoạt động trở lại trên môi trường mạng. - Kiểm thử toàn bộ hệ thống sau khi khắc phục sự cố; theo dõi, giám sát thường xuyên, ngăn chặn khả năng sự cố lặp lại hoặc xảy ra tương tự trong quá trình khôi phục.	Văn phòng Sở, các đơn vị chuyên môn, trực thuộc quản lý, vận hành hệ thống thông tin	Công an tỉnh; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (UCKCSC); Đơn vị cung cấp dịch vụ an toàn thông tin mạng

STT	Quy trình	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp
III	**Tổng kết**			
1	Tổng kết và báo cáo tình hình	Tổng kết, báo cáo toàn diện sự cố đến Công an tỉnh và Đội UCKCSC (*theo mẫu tại Phụ lục 3*).	Văn phòng Sở, các đơn vị chuyên môn, trực thuộc quản lý, vận hành hệ thống thông tin	Công an tỉnh; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (UCKCSC); Đơn vị cung cấp dịch vụ an toàn thông tin mạng

PHỤ LỤC 2

Báo cáo ban đầu sự cố an toàn thông tin mạng của Hệ thống thông tin (HTTT)

(ban hành kèm theo Kế hoạch số: 39 /KH-SCT ngày 22/5/2025 của Sở Công Thương)

I. Thông tin về tổ chức/cá nhân báo cáo sự cố

1. Tên tổ chức/cá nhân báo cáo sự cố:……..

2. Địa chỉ:…….

3. Điện thoại:……..; Email:……

II. Người liên hệ

1. Họ tên:……..; Chức vụ:…….

2. Điện thoại:……..; Email:……

III. Thông tin chi tiết về hệ thống bị sự cố

Tên đơn vị đang quản lý, vận hành HTTT	*Điền tên đơn vị đang quản lý, vận hành hoặc được thuê quản lý, vận hành HTTT*
Cơ quan chủ quản HTTT	*Điền tên cơ quan chủ quản*
Tên HTTT xảy ra sự cố	*Điền tên hệ thống bị sự cố, tên miền, địa chỉ IP liên quan*
Phân loại cấp độ HTTT	☐ Cấp độ 1 ☐Cấp độ 2 ☐Cấp độ 3 ☐Cấp độ 4 ☐Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin	*Điền tên nhà cung cấp dịch vụ an toàn thông tin*
Tên nhà cung cấp dịch vụ kết nối bên ngoài	*Điền tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)*
Dải IP Public kết nối hệ thống bên ngoài	*Điền thông tin dải IP công khai kết nối với hệ thống ra bên ngoài*

IV. Mô tả sơ bộ về sự cố

Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:……

1. Ngày phát hiện sự cố: dd/mm/yyyy

2. Thời gian phát hiện sự cố:……giờ…….phút……..giây……..

3. Hiện trạng sự cố: ☐Đã được xử lý ☐Chưa được xử lý

4. Cách thức phát hiện:

☐Qua hệ thống phát hiện xâm nhập ☐Kiểm tra dữ liệu lưu lại (log file)

☐Nhận được thông báo từ……

☐Nội dung khác……..

5. Đã gửi thông báo sự cố cho:

☐Thành viên Đội UPKCSC ☐Công an tỉnh

☐Đơn vị xây dựng, phát triển hệ thống, dịch vụ, cổng/trang thông tin điện tử……

☐Cơ quan chức năng có liên quan khác……

6. Thông tin bổ sung về hệ thống xảy ra sự cố:

a) Hệ điều hành:……; Phiên bản:…….

b) Các dịch vụ có trên hệ thống: (*đánh dấu những dịch vụ có trên hệ thống*)

☐Web Server ☐Mail Server ☐Database Server

☐Dịch vụ khác……

c) Các giải pháp an toàn thông tin đã triển khai: (*đánh dấu những giải pháp*)

☐Antivirus ☐Firewall ☐Phòng chống xâm nhập

☐Giải pháp khác……..

d) Các địa chỉ IP của hệ thống:……

e) Các tên miền của hệ thống:……..

f) Mục đích chính của hệ thống:…….

g) Thông tin gửi kèm: (*đánh dấu những dịch vụ có trên hệ thống*)

☐Nhật ký hệ thống ☐Mẫu virus, mã độc ☐Danh sách IP

☐Thông tin khác……..

h) Thông tin cung cấp trong thông báo sự cố này phải giữ bí mật: ☐Có; ☐Không

V. Kiến nghị, đề xuất hỗ trợ

Mô tả tóm lược về kiến nghị, đề xuất được hỗ trợ (nếu có)…….

VI. Thời gian thực hiện báo cáo sự cố: ……/……/……/…../……../……(*ngày/tháng/năm/giờ/phút*)

CÁ NHÂN ĐẠI DIỆN THEO PHÁP LUẬT

(Ký tên, đóng dấu)

PHỤ LỤC 3

Báo cáo kết thúc ứng phó sự cố an toàn thông tin mạng

(ban hành kèm theo Kế hoạch số: /KH-SCT ngày /5/2025 của Sở Công Thương)

I. Thông tin về tổ chức/cá nhân báo cáo sự cố

1. Tên tổ chức/cá nhân báo cáo sự cố:……..

2. Địa chỉ:…….

3. Điện thoại:……..; Email:……

II. Ký hiệu báo cáo ban đầu sự cố: Số ký hiệu/Ngày báo cáo (*dd/mm/yyyy*):……

III. Thông tin chi tiết về hệ thống bị sự cố

Tên đơn vị đang quản lý, vận hành HTTT	*Điền tên đơn vị đang quản lý, vận hành hoặc được thuê quản lý, vận hành HTTT*
Cơ quan chủ quản HTTT	*Điền tên cơ quan chủ quản*
Tên HTTT xảy ra sự cố	*Điền tên hệ thống bị sự cố, tên miền, địa chỉ IP liên quan*
Phân loại cấp độ HTTT	☐ Cấp độ 1 ☐Cấp độ 2 ☐Cấp độ 3 ☐Cấp độ 4 ☐Cấp độ 5

IV. Tên/Mô tả sơ bộ về sự cố

Tóm tắt ngắn gọn về sự cố, diễn biến mức độ, phạm vi ảnh hưởng…….

1. Ngày phát hiện sự cố (dd/mm/yyyy):……..

2. Thời gian phát hiện sự cố:……..giờ……..phút……..giây…….

V. Các tài liệu đính kèm

Liệt kê, thống kê các tài liệu, báo cáo liên quan (tập tin, văn bản, hình ảnh, phương án xử lý, log file)……..

CÁ NHÂN ĐẠI DIỆN THEO PHÁP LUẬT

(Ký tên, đóng dấu)