

Số: /KH-SKHCN

Khánh Hòa, ngày 08 tháng 12 năm 2023

KẾ HOẠCH

Ứng phó sự cố an toàn thông tin mạng của Sở Khoa học và Công nghệ năm 2024

Thực hiện Kế hoạch số 12830/KH-UBND ngày 04/12/2023 của Ủy ban nhân dân tỉnh Khánh Hòa về việc ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2024, Sở Khoa học và Công nghệ ban hành Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng với những nội dung như sau:

I. MỤC ĐÍCH YÊU CẦU

1. Mục đích:

- Đảm bảo an toàn thông tin cho các hệ thống thông tin của Sở Khoa học và Công nghệ đảm bảo khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng, đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

- Nâng cao năng lực giám sát nhằm tăng cường khả năng phát hiện sớm, cảnh báo kịp thời, chính xác về các sự kiện, rủi ro, dấu hiệu, hành vi, mức độ xâm hại, nguy cơ, điểm yếu, lỗ hổng gây mất an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ chính phủ điện tử của Sở.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với lực lượng công chức, viên chức và người lao động trong toàn ngành.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu sự cố bảo đảm an toàn thông tin mạng của Sở.

2. Yêu cầu:

- Căn cứ trên kết quả khảo sát, đánh giá các nguy cơ, sự cố mất an toàn thông tin mạng của Sở để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp.

- Phương án đối phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra

được các tiêu chí để có thể nhanh chóng xác định tính chất, mức độ nghiêm trọng khi có sự cố xảy ra.

- Xác định cụ thể các nguồn lực, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, đảm bảo khả thi, đạt hiệu quả.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác đảm bảo an toàn thông tin giữa Sở với các cơ quan nhà nước trên địa bàn tỉnh; giữa Sở với các đơn vị trực thuộc Sở và sự phối hợp, hỗ trợ của các đơn vị nghiệp vụ của Sở Thông tin và Truyền thông, Bộ Thông tin và Truyền thông.

II. NHIỆM VỤ TRIỂN KHAI

1. Triển khai các nhiệm vụ khi chưa có sự cố xảy ra

1.1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng

Nội dung thực hiện: Tổ chức tuyên truyền, phổ biến, hướng dẫn nội dung của Luật An toàn thông tin mạng; Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ; Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Thủ tướng Chính phủ; Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ; Chỉ thị số 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ; Kế hoạch số 13784/KH-UBND ngày 31/12/2020 của UBND tỉnh Khánh Hòa và các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng trên các phương tiện thông tin đại chúng, trên Cổng Thông tin điện tử của tỉnh, Trang thông tin điện tử của các sở, ban, ngành và của Sở Khoa học và Công nghệ.

- Đơn vị thực hiện: Sở Khoa học và Công nghệ, các đơn vị trực thuộc.

- Đơn vị phối hợp: Các sở, ban, ngành, Công an tỉnh, UBND các huyện, thị xã, thành phố và các đơn vị có liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

1.2. Triển khai các chương trình đào tạo, bồi dưỡng kỹ năng đánh giá, ứng phó sự cố

- Nội dung thực hiện: Phối hợp với Sở Thông tin và Truyền thông tổ chức

huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; đào tạo nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố; tham gia huấn luyện, đào tạo, bồi dưỡng, diễn tập vùng, miền, quốc gia theo triệu tập của Sở Thông tin và Truyền thông, Bộ Thông tin và Truyền thông.

- Đơn vị thực hiện: Sở Khoa học và Công nghệ, các đơn vị trực thuộc.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa và các đơn vị có liên quan.

- Thời gian thực hiện: Trong năm 2024.

1.3. Triển khai phòng ngừa sự cố, giám sát phát hiện sớm sự cố

Nội dung thực hiện: Tổ chức giám sát, phát hiện sớm các nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro an toàn thông tin mạng, phần mềm độc hại; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

Rà soát đánh giá tình hình, công tác phòng ngừa sự cố trong thời gian qua, xác định những mặt trọng tâm, trọng điểm có nguy cơ, từ đó tập trung triển khai các biện pháp bảo vệ, phòng ngừa; chú ý sắp xếp, bố trí cán bộ đủ năng lực chuyên môn, có phẩm chất tốt để đảm nhiệm những vị trí quan trọng trong quản lý, vận hành các hệ thống thông tin. Chú trọng vấn đề nâng cấp giao thức bảo mật cho các trang/cổng thông tin điện tử, cơ sở hạ tầng mạng trong hệ thống thông tin của Sở và các đơn vị trực thuộc.

- Đơn vị thực hiện: Sở Khoa học và Công nghệ, các đơn vị trực thuộc.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa và các đơn vị có liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

1.4. Triển khai các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

- Nội dung thực hiện: Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện; mua mới, gia hạn bản quyền phần mềm phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng các nguồn lực và tài chính để sẵn

sàng đôi phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của đội ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- Đơn vị thực hiện: Sở Khoa học và Công nghệ, các đơn vị trực thuộc.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa và các đơn vị có liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

1.5. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

- Nội dung thực hiện: Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng đối với hệ thống thông tin của Sở và các đơn vị trực thuộc Sở; đánh giá, dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra với hệ thống thông tin; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực phục vụ đối phó, ứng cứu, khắc phục sự cố của cơ quan, đơn vị (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

- Đơn vị thực hiện: Sở Khoa học và Công nghệ, các đơn vị trực thuộc.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa, các nhà thầu cung cấp dịch vụ an toàn thông tin mạng (nếu có) và các đơn vị có liên quan.

- Thời gian thực hiện: Kiểm tra hệ thống thông tin định kỳ 06 tháng/01 lần.

1.6. Xây dựng phương án đối phó, ứng cứu đối với một số tình huống sự cố

- Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp.

- Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống.

- Đơn vị chủ trì: Sở Khoa học và Công nghệ.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia

(Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); các đơn vị liên quan khác.

2. Triển khai các nhiệm vụ khi có sự cố xảy ra

Thực hiện theo Quy trình ứng cứu, xử lý khẩn cấp sự cố tấn công mạng tại **Phụ lục I** kèm theo Kế hoạch này.

III. KINH PHÍ THỰC HIỆN

Căn cứ Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ trưởng Bộ Tài chính quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện công tác ứng cứu sự cố, đảm bảo an toàn thông tin.

IV. TỔ CHỨC THỰC HIỆN

1. Các đơn vị trực thuộc Sở

- Phân công lãnh đạo phụ trách và thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về an toàn thông tin mạng của đơn vị.

- Tích cực phối hợp với Sở Khoa học và Công nghệ trong việc thực hiện các nhiệm vụ được giao tại Kế hoạch này.

- Định kỳ hằng năm, gửi báo cáo tình hình, kết quả về Sở Khoa học và Công nghệ để tổng hợp báo cáo UBND tỉnh hoặc báo cáo đột xuất khi có yêu cầu.

2. Văn phòng Sở

- Là thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng của tỉnh; làm đầu mối, tổ chức hoạt động ứng cứu sự cố, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh; tham gia hoạt động ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng tỉnh khi có yêu cầu từ Cơ quan thường trực hoặc Cơ quan điều phối.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát công tác bảo đảm an toàn thông tin định kỳ hằng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh.

- Theo dõi, hướng dẫn, kiểm tra, giám sát việc thực hiện ứng phó sự cố đảm bảo an toàn thông tin mạng ở các đơn vị trực thuộc.

3. Các phòng thuộc Sở

Căn cứ vào chức năng, nhiệm vụ, tổ chức thực hiện kế hoạch hoạt động, đảm bảo thực hiện nhiệm vụ an toàn thông tin mạng trong phạm vi quản lý phù hợp với điều kiện thực tế.

Trên đây là Kế hoạch Ứng phó sự cố đảm bảo an toàn thông tin mạng tại Sở Khoa học và Công nghệ năm 2024, yêu cầu các đơn vị trực thuộc căn cứ Kế hoạch này triển khai thực hiện tại đơn vị. Trong quá trình thực hiện nếu có vướng mắc, khó khăn, các đơn vị phản ánh, kiến nghị về Văn phòng Sở để tổng hợp báo cáo Sở Thông tin và Truyền thông./.

Nơi nhận:

- Sở Thông tin và Truyền thông;
 - Lãnh đạo Sở (theo dõi);
 - Các phòng thuộc Sở;
 - Các đơn vị trực thuộc;
 - Lưu: VT, VP.
- } (VBĐT);

**KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC**

Lê Phước Đức

PHỤ LỤC I
QUY TRÌNH ỨNG CỨU, XỬ LÝ KHẨN CẤP SỰ CỐ TẤN CÔNG MẠNG
(Ban hành kèm theo Kế hoạch số /KH-SKHCN ngày /12/2023 của Sở Khoa học và Công nghệ)

Stt	Quy trình	Nội dung thực hiện	Đơn vị chủ trì	Đơn vị phối hợp
I	Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố			
1.	Tiếp nhận, xác minh sự cố	Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể xảy ra từ các nguồn bên trong và bên ngoài. Khi phân tích, xác minh sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố.	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC).
2.	Triển khai các bước ưu tiên ứng cứu ban đầu	Căn cứ vào bản chất, dấu hiệu của sự cố tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo Kế hoạch Ứng phó sự cố đã được cấp thẩm quyền phê duyệt hoặc theo hướng dẫn của Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh hoặc Cơ quan điều phối quốc gia.	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
3.	Triển khai lựa chọn phương án ứng cứu	Căn cứ theo Kế hoạch Ứng phó sự cố đã được UBND tỉnh ban hành hoặc theo hướng dẫn của Cơ quan thường trực ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh để lựa chọn phương án ngăn chặn và xử lý sự cố; báo cáo, đề xuất Chủ quản hệ thống thông tin hoặc Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa để xin ý kiến chỉ đạo (nếu cần thiết).	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
4.	Chỉ đạo xử lý sự cố (trong	Căn cứ theo báo cáo, đề xuất của Đơn vị quản lý, vận hành hệ thống thông tin, Ban Chỉ đạo Chuyển	Ban Chỉ đạo chuyển đổi số tỉnh Khánh	Đơn vị quản lý, vận hành hệ thống thông tin

	trường hợp sự cố nghiêm trọng, cần triệu tập Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa và đề nghị Cơ quan điều phối quốc gia hỗ trợ)	đổi số tỉnh Khánh Hòa phối hợp chủ quản hệ thống thông tin và tham khảo ý kiến Cơ quan điều phối quốc gia (nếu cần) thực hiện chỉ đạo Cơ quan chuyên trách ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa triển khai công tác ứng cứu, xử lý.	Hòa	
5.	Báo cáo sự cố	Sau khi đã triển khai các bước ưu tiên ứng cứu ban đầu, đơn vị quản lý, vận hành hệ thống thông tin tổ chức thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan theo quy định tại Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc và quy định nội bộ (nếu có).	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
6.	Điều phối công tác ứng cứu	Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của đơn vị quản lý, vận hành hệ thống thông tin, Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa, Cơ quan điều phối quốc gia hoặc Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ứng cứu sự cố.	Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa; Cơ quan điều phối quốc gia; Sở Thông tin và Truyền thông.	Sở Khoa học và Công nghệ, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.
II	Triển khai ứng cứu, ngăn chặn và xử lý sự cố			

1	Triển khai ứng cứu, ngăn chặn và xử lý sự cố	Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng; phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.	Đơn vị quản lý, vận hành hệ thống thông tin; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng	Sở Thông tin và Truyền thông; Cơ quan điều phối quốc gia.
III	Xử lý sự cố, gỡ bỏ, khôi phục và xử lý vi phạm			
1.	Xử lý, gỡ bỏ sự cố	Sau khi đã triển khai ngăn chặn sự cố, đơn vị quản lý, vận hành hệ thống thông tin chịu trách nhiệm khẩn trương ngăn chặn sự cố, đồng thời tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin (phối hợp với Sở Thông tin và Truyền thông và Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh nếu cần thiết).	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
2.	Khôi phục sự cố	Đơn vị quản lý, vận hành hệ thống thông tin chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục hệ thống thông tin, dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin của hệ thống thông tin.	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
3.	Kiểm tra, đánh giá an toàn hệ thống thông tin sau khi khôi phục	Đơn vị quản lý, vận hành hệ thống thông tin và các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa đảm bảo an toàn, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức ứng cứu để xử lý dứt điểm, khôi phục hoạt động của hệ thống thông tin trở lại bình thường.	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cục phòng chống tội phạm sử dụng công nghệ cao (Bộ Công an); Cơ quan điều phối quốc gia.
IV	Tổng kết, đánh giá			
1	Tổng kết, đánh	Đơn vị quản lý, vận hành hệ thống thông tin bị sự	Đơn vị quản lý, vận	Sở Thông tin và Truyền thông;

	giá	cố phối hợp với Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh và Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa triển khai tổng hợp toàn bộ các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ứng cứu sự cố, báo cáo Chủ quản hệ thống thông tin, Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa và Cơ quan điều phối quốc gia; tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai.	hành hệ thống thông tin	Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa; Cơ quan điều phối quốc gia.
--	-----	--	-------------------------	---