UBND TỈNH KHÁNH HÒA **SỞ TÀI CHÍNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 6031 /KH-STC	*Khánh Hòa, ngày 22 tháng 12 năm 2023*

KẾ HOẠCH

Ứng phó sự cố, bảo đảm an toàn thông tin mạng của Sở Tài chính năm 2024

Thực hiện Kế hoạch số 12830/KH-UBND ngày 04/12/2023 của UBND tỉnh Khánh Hòa về ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2024, Sở Tài chính xây dựng kế hoạch với những nội dung như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Đảm bảo an toàn thông tin cho hệ thống thông tin của cơ quan; 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 an toàn thông tin mạng của cơ quan để 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 các hệ thống, dịch vụ công nghệ thông tin phục vụ chính phủ điện tử của cơ quan.

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

2. Yêu cầu

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

- Có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi xảy ra;

- Xác định cụ thể các nguồn lực đảm bảo, giải pháp tổ chức triển khai khả thi, hiệu quả các nội dung của Kế hoạch.

II. NỘI DUNG THỰC HIỆN

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

1.1. Công tác tuyên truyền, phổ biến

- 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 ban hành Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 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 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Chỉ thị số 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát; Kế hoạch số 13784/KH-UBND ngày 31/12/2020 của UBND tỉnh Khánh Hòa về ứng dụng công nghệ thông tin, phát triển chính quyền số và bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa giai đoạn 2021 - 2025 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, cổng Thông tin điện tử của tỉnh, Trang thông tin điện tử của sở.

1.2. Tham gia các chương trình huấn luyện, đào tạo, bồi dưỡng, diễn tập

Phối hợp với Sở Thông tin và Truyền thông tham gia 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, quốc tế.

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

Phối hợp với Sở Thông tin và Truyền thông hoặc các đơn vị chuyên trách kiểm tra, giám sát, phát hiện sớm các nguy cơ, sự cố; 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 bảo 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.

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

Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, 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 sàn đối phó, ứng cứu, khắc phục khi sự cố xảy ra;

thuê dịch vụ kỹ thuật và tổ chức, tham gia các hoạt động của mạng lưới ứng cứu sự cố.

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

Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng đối với hệ thống thông tin; đánh giá, dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra với hệ thống thông tin; dự báo đối tượng có thể tấn công, phá hoại gây ra sự cố mất an toàn thông tin mạng; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể nếu có 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 (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

1.6. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Chủ động xây dựng, hoàn thiện, thường xuyên cập nhật vào hệ thống theo cấp độ an toàn thông tin đã được phê duyệt đối với các tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu đối với một số sự cố cụ thể, phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng khi sự cố xảy ra.

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

2.1. Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố

a) Tiếp nhận, xác minh sự cố:

- CBCC các phòng thuộc Sở khi phát hiện sự cố cần báo ngay cho quản trị mạng để theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố đó có thể từ các nguồn bên trong và bên ngoài, phân tích, xác minh sự cố đã xảy ra, ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố.

b) Triển khai các bước ưu tiên ứng cứu ban đầu:

- Căn cứ vào bản chất, dấu hiệu của sự cố để 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.

c) Triển khai lựa chọn phương án ứng cứu:

- Căn cứ 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 để lựa chọn phương án ngăn chặn và xử lý sự cố.

d) Báo cáo sự cố:

- Sau khi đã triển khai các bước ưu tiên ứng cứu ban đầu, 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 các hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

2.2. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

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. Kịp thời thông báo cho Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa nếu sự cố ngoài phạm vi kiểm soát.

2.3. Xử lý sự cố, gỡ bỏ và khôi phục

a) Xử lý sự cố:

- Sau khi đã triển khai ngăn chặn sự cố, triển khai 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 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 cho hệ thống thông tin.

b) Khôi phục:

- Phối hợp với Sở Thông tin và Truyền thông 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.

c) Kiểm tra, đánh giá hệ thống thông tin:

- 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 hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân để dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.

2.4. Tổng kết, đánh giá

Tổng hợp toàn bộ các thông tin, báo cáo, phân tích có liên quạn đến sự cố, công tác triển khai phương án ứng cứu sự cố, báo cáo và 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 có thể xảy ra trong tương lai.

III. TỔ CHỨC THỰC HIỆN

1. Văn phòng Sở

- Chịu trách nhiệm đăng tải trên Cổng thông tin điện tử của Sở; gửi qua E-Office để CBCC được biết, thực hiện các Kế hoạch, văn bản có liên quan;

- Tổ chức tuyên truyền, phổ biến kịp thời vào thứ Năm hàng tuần;

- Hàng năm kiểm tra, tham mưu đề xuất việc mua sắm, trang bị, nâng cấp các thiết bị, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố; chuẩn bị

các điều kiện bảo đảm để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; Tham mưu việc mua sắm, sử dụng phần mềm có bản quyền trong hoạt động của cơ quan;

- Đánh giá, kiểm tra hệ thống thông tin định kỳ 06 *tháng (trước ngày 10 tháng 6), 01 năm (trước ngày 05 tháng 12).*

- Hàng ngày thực hiện sao lưu dữ liệu chung của Sở, đảm bảo an toàn dữ liệu;

- Phối hợp với Sở Thông tin và Truyền thông kiểm tra, đánh giá, khắc phục sự cố an toàn thông tin mạng khi có sự cố xảy ra;

- Cử CBCC tham gia đầy đủ các lớp huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố.

- Thường xuyên cập nhật, bổ sung vào hệ thống cấp độ an toàn thông tin, gửi Sở Thông tin và Truyền thông thẩm định khi có thay đổi bên trong hệ thống.

2. Các phòng nghiệp vụ thuộc Sở

Lãnh đạo các phòng thường xuyên nhắc nhở các CBCC trong phòng tuân thủ nghiêm các quy định về sử dụng, vận hành các ứng dụng và các thiết bị tin học tại cơ quan, kịp thời thông báo cho quản trị mạng ngay khi phát hiện sự cố mất an toàn thông tin mạng; thường xuyên thực hiện sao lưu dữ liệu vào ổ đĩa dùng chung của phòng; đề xuất, kiến nghị những giải pháp nhằm đảm bảo an toàn thông tin mạng trong cơ quan./.

Nơi nhận: (VBĐT)
- Sở TT&TT;
- Các phòng thuộc Sở;
- Lưu: VT, VP.

GIÁM ĐỐC

SỞ TÀI CHÍNH

Trần Thông