UBND TỈNH KHÁNH HÒA
SỞ TÀI NGUYÊN VÀ MÔI TRƯỜNG

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

Số: 706/KH-STNMT

Khánh Hòa, ngày 23 tháng 02 năm 2018

KẾ HOẠCH
Ứng phó sự cố đảm bảo an toàn thông tin mạng Sở Tài nguyên và Môi trường năm 2018

Triển khai Kế hoạch 439/KH-UBND ngày 11 tháng 01 năm 2018 của UBND tỉnh Khánh Hòa về Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2018. Sở Tài nguyên và Môi trường xây dựng và ban hành Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng trong Sở Tài nguyên và Môi trường năm 2018 với nội dung như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

a) Đảm bảo an toàn thông tin mạng của ngành tài nguyên và môi trường Khánh Hòa; 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.

b) Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với lực lượng cán bộ, công chức, viên chức.

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

2. Yêu cầu

a) Phải khảo sát, đánh giá các nguy cơ, sự cố an toàn thông tin mạng của toàn hệ thống để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp.

b) 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 được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra.

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

II. NHIỆM VỤ TRIỂN KHAI

1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật; tập huấn nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng

- Tổ chức tuyên truyền, phổ biến qua hệ thống EO và Cổng thông tin điện tử của Sở Tài nguyên và Môi trường các văn bản: 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; Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020; 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 và các văn bản quy phạm pháp luật về an toàn thông tin mạng.

- Đơn vị chủ trì: Văn phòng Sở, Trung tâm Công nghệ thông tin

- Đơn vị phối hợp: Các phòng, đơn vị trực thuộc Sở Tài nguyên và Môi trường

- Thời gian thực hiện: Thường xuyên trong năm.

2. 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 của các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố *(bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).*

- Đơn vị thực hiện: Trung tâm Công nghệ thông tin, các đơn vị trực thuộc.

- Đơn vị phối hợp: Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh; Nhà thầu cung cấp dịch vụ an toàn thông tin mạng *(nếu có)*; các đơn vị liên quan khác.

- Thời gian thực hiện: Thường xuyên trong năm.

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

Đối với mỗi hệ thống thông tin, chương trình, ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

a) 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

- Sự cố do bị tấn công mạng;

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...;

- Sự cố do lỗi của người quản trị, vận hành hệ thống;

- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v...

b) Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tình huống sau:

- Tình huống sự cố do bị tấn công mạng:

+ Tấn công từ chối dịch vụ;

+ Tấn công giả mạo;

+ Tấn công sử dụng mã độc;

+ Tấn công truy cập trái phép, chiếm quyền điều khiển;

+ Tấn công thay đổi giao diện;

+ Tấn công mã hóa phần mềm, dữ liệu, thiết bị;

+ Tấn công phá hoại thông tin, dữ liệu, phần mềm;

+ Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;

+ Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;

+ Các hình thức tấn công mạng khác.

- Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:

+ Sự cố nguồn điện;

+ Sự cố đường kết nối Internet;

+ Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;

+ Sự cố liên quan đến quá tải hệ thống;

+ Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống:

+ Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;

+ Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;

+ Lỗi liên quan đến chính sách và thủ tục an toàn thông tin;

+ Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;

+ Lỗi khác liên quan đến người quản trị, vận hành hệ thống.

- Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v....

c) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, giữa các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố;

d) Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ, và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể.

- Đơn vị chủ trì: Văn phòng Sở, Trung tâm Công nghệ thông tin, các đơn vị trực thuộc.

- Đơn vị phối hợp: Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh; Nhà thầu cung cấp dịch vụ an toàn thông tin mạng (nếu có); các đơn vị liên quan khác.

- Thời gian thực hiện: Thường xuyên trong năm.

4. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố

Triển khai các hoạt động thuộc trách nhiệm của các cơ quan, đơn vị liên quan theo quy định tại các Điều 11, Điều 12, Điều 13, Điều 14 và các nội dung liên quan khác của Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia *(sau đây gọi tắt là Quyết định số 05/2017/QĐ-TTg).*

Dự phòng kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng cứu sự cố; triển khai điều hành phối hợp tổ chức ứng cứu và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố khi có sự cố xảy ra.

a) Báo cáo sự cố an toàn thông tin mạng theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg

- Đơn vị thực hiện:

+ Trung tâm Công nghệ thông tin, các đơn vị trực thuộc báo cáo Sở Tài nguyên và Môi trường Khánh Hòa, đồng gửi Sở Thông tin và Truyền thông Khánh Hòa;

+ Sở Tài nguyên và Môi trường báo cáo Ban chỉ đạo CNTT tỉnh và Cơ quan điều phối quốc gia;

- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

b) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg

- **Đơn vị chủ trì:** Trung tâm Công nghệ thông tin, các đơn vị trực thuộc;

- **Đơn vị phối hợp:** Cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp máy tính Việt Nam -VNCERT); Ban chỉ đạo CNTT tỉnh; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; đơn vị cung cấp dịch vụ an toàn thông tin mạng (nếu có); các đơn vị chức năng liên quan.

- **Thời gian thực hiện:** Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố của tổ chức, cá nhân.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg

5. Triển khai huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố, cụ thể bao gồm:

a) Triển khai các chương trình huấn luyện, diễn tập

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; huấn luyện, diễn tập 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, diễn tập vùng, miền, quốc gia, quốc tế.

- **Đơn vị chủ trì:** Trung tâm Công nghệ thông tin; Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh.

- **Đơn vị phối hợp:** Văn phòng Sở, các phòng, đơn vị trực thuộc; Cơ quan điều phối quốc gia *(Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - VNCERT)*; các đơn vị chức năng liên quan.

- **Thời gian thực hiện:** Hàng năm.

b) Các nội dung, nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố

Giám sát, phát hiện sớm 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.

- **Đơn vị chủ trì:** Trung tâm Công nghệ thông tin; các đơn vị trực thuộc;

- Đơn vị phối hợp: Sở Thông tin và Truyền thông; Cơ quan điều phối quốc gia *(Trung tâm ứng cứu khẩn cấp máy tính Việt Nam -VNCERT);* các đơn vị chức năng liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

c) Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, 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 đối 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 chủ trì: Văn phòng Sở, Trung tâm Công nghệ thông tin, các đơn vị trực thuộc Sở.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông; Cơ quan điều phối quốc gia *(Trung tâm ứng cứu khẩn cấp máy tính Việt Nam -VNCERT)*; các đơn vị chức năng liên quan.

- Thời gian thực hiện: Hàng năm.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện được sử dụng từ nguồn ngân sách.

IV. TỔ CHỨC THỰC HIỆN

1. Các cơ quan, đơn vị trực thuộc;

- Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch ứng dụng công nghệ thông tin hàng năm của cơ quan, đơn vị mình để triển khai các nhiệm vụ được giao tại Kế hoạch này.

- 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 cơ quan, đơn vị.

- Thực hiện xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 và Điều 15 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 và theo hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Định kỳ hằng năm, gửi báo cáo tình hình, kết quả về Sở Tài nguyên và Môi trường để tổng hợp báo cáo UBND tỉnh hoặc báo cáo đột xuất khi cấp trên có yêu cầu.

2. Trung tâm Công nghệ thông tin

- 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.

- Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo thẩm quyền quy định tại Khoản 1, Khoản 2 Điều 12 và Khoản 5 Điều 15 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 và theo hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/04/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

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

3. Các phòng, đơn vị thuộc Sở

Căn cứ vào chức năng, nhiệm vụ, tổ chức thực hiện kế hoạch hoạt động, đảm bảo thực hiện nhiệm vụ bảo đảm 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 Sở Tài nguyên và Môi trường Khánh Hòa, yêu cầu Thủ trưởng các Cơ quan, đơn vị trực thuộc triển khai thực hiện. Trong quá trình thực hiện nếu có vướng mắc, khó khăn, các cơ quan, đơn vị phản ánh, kiến nghị về Sở Tài nguyên và Môi trường để tổng hợp báo cáo UBND tỉnh./.

GIÁM ĐỐC

Võ Tấn Thái

Nơi nhận:
- Sở Thông tin & Truyền thông *(VBĐT)*;
- Lãnh đạo Sở (VBĐT);
- Các phòng thuộc Sở (VBĐT);
- Các cơ quan, đơn vị trực thuộc (VBĐT);
- Lưu: VT, TTCNTT.