UBND TỈNH KHÁNH HÒA
BAN QUẢN LÝ DỰ ÁN PHÁT TRIỂN TỈNH KHÁNH HÒA

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

Số: 476 /KH-BQL

Khánh Hòa, ngày 22 tháng 5 năm 2019

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa năm 2019

Căn cứ Kế hoạch số 3669/KH-UBND ngày 19/4/2019 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 năm 2019;

Thực hiện Công văn số 753/STTTT-CNTT ngày 02/5/2019 của Sở Thông tin và Truyền thông tỉnh Khánh Hòa về việc triển khai thực hiện Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh năm 2019. Ban Quản lý dự án Phát triển tỉnh Khánh Hòa xây dựng Kế hoạch triển khai thực hiện như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Tập trung đảm bảo an toàn thông tin cho các hệ thống thông tin quan trọng của cơ quan, đảm bảo các 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 nhận thức, kiến thức về an toàn thông tin cho toàn thể cán bộ, công chức, viên chức. 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 khẩn cấp sự cố bảo đảm an toàn thông tin mạng.

2. Yêu cầu

- Dựa trên tình hình thực tế, kết quả khảo sát, đánh giá các nguy cơ, sự cố mất an toàn thông tin mạng của các hệ thống thông tin của cơ quan, đơn vị trong thời gian qua, để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời và phù hợp.

- Các phương án đưa ra nhằm đối phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra được các tiêu chí rõ ràng để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng khi sự cố xảy ra.

- 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. NỘI DUNG TRIỂN KHAI

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

1.1 Tuyên truyền, phổ biến Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 và các văn bản quy phạm pháp luật về an toàn thông tin mạng

- Nội dung thực hiện: Tổ chức tuyên truyền, phổ biến trên E-Office, Trang thông tin điện tử tổng hợp của Ban (http://kdpm.khanhhoa.gov.vn) về 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; Kế hoạch số 3669/KH-UBND ngày 19/4/2019 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 năm 2019 và các văn bản quy phạm pháp luật về an toàn thông tin mạng.

- Đơn vị chủ trì thực hiện: Phòng Môi trường xã hội.

- Đơn vị phối hợp: Phòng TCHC và các phòng chuyên môn.

- Thời gian thực hiện: Trong năm 2019.

1.2 Tuyên truyền, phổ biến Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ tài chính Quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng

- Nội dung thực hiện: Tổ chức tuyên truyền, phổ biến trên E-Office, Trang thông tin điện tử tổng hợp của Ban (http://kdpm.khanhhoa.gov.vn) về Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ tài chính Quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng

- Đơn vị chủ trì thực hiện: Phòng Môi trường xã hội.

- Đơn vị phối hợp: Phòng TCHC và các phòng chuyên môn.

- Thời gian thực hiện: Trong năm 2019

1.3. Phối hợp tham gia các phương án, chương trình huấn luyện, đào tạo, bồi dưỡng, diễn tập

- Nội dung thực hiện: Phối hợp tham gia huấn luyện, đào tạo, bồi dưỡng, diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể do các cơ quan chuyên môn thực hiện; huấn luyện, đào tạo, bồi dưỡng, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố.

- Đơn vị chủ trì thực hiện: Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh (Sở Thông tin và Truyền thông); Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.

- Thời gian thực hiện: Theo quy định.

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

- Nội dung thực hiện: 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.

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

- Thời gian thực hiện: Định kỳ hàng quý.

1.5. 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, gia hạn bản quyền các phần mềm; 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; thuê dịch vụ kỹ thuật, chuyên gia ứng cứu sự cố và sự hỗ trợ, phối hợp của các cơ quan, đơn vị liên quan khi tổ chức tham gia các hoạt động ứng cứu sự cố.

- Đơn vị chủ trì thực hiện: Phòng TCHC và cán bộ phụ trách công nghệ thông tin

- Đơn vị phối hợp: Phòng Tài chính kế toán và các phòng chuyên môn.

- Thời gian thực hiện: 6 tháng và hàng năm.

1.6. Kiểm tra, đánh giá các nguy cơ, sự cố an toàn thông tin mạng

- Nội dung thực hiện: Tổ chức kiểm tra, đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của 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; 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, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (*bao gồm của các nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có*).

- Đơn vị chủ trì thực hiện: Phòng TCHC và cán bộ phụ trách công nghệ thông tin

- Đơn vị phối hợp: Các phòng chuyên môn.

- Thời gian thực hiện: Định kỳ hàng quý.

1.7. Xây dựng các phương án đối phó, ứng cứu; dự báo, đưa ra các biện pháp khắc phục đối với một số tình huống sự cố cụ thể

- Nội dung thực hiện: 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. Các đơn vị sử dụng, vận hành hệ thống thông tin, chương trình ứng dụng phải xây dựng phương án đối phó, ứng cứu sự cố.

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 thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

- Thời gian thực hiện: Thường xuyên trong năm.

2. Triển khai các nhiệm vụ, biện pháp khắc phục 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:

- Nội dung thực hiện: 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 minh nguồn gốc sự cố.

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

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

- Nội dung thực hiện: Sau khi xác định sự cố xảy ra, đơn vị sử dụng, vận hành hệ thống thông tin căn cứ vào dấu hiệu, cảnh báo, hướng dẫn của cơ quan chuyên môn để 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 làm theo hướng dẫn của cơ quan chuyên trách ứng cứu sự cố an toàn thông tin trên địa bàn tỉnh.

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

c) Triển khai lựa chọn các phương án ứng cứu:

- Nội dung thực hiện: Căn cứ theo Kế hoạch ứng phó sự cố của cơ quan và cấp có thẩm quyền phê duyệt hoặc theo các cảnh báo, hướng dẫn của cơ quan chuyên trách 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 đơn vị quản lý hệ thống thông tin để xin ý kiến chỉ đạo nếu cần.

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

d) Báo cáo sự cố:

- Nội dung thực hiện: Sau khi đã triển khai các bước ưu tiên ứng cứu ban đầu, đơn vị quản lý, sử dụng, 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, tổ chức theo quy định tại Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12/09/2017 và quy định nội bộ (nếu có).

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

e) Công tác phối hợp trong ứng cứu:

- Nội dung thực hiện: Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của các đơn vị sử dụng, vận hành hệ thống thông tin và cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng, các cơ quan, đơn vị liên quan tích cực thực hiện công tác phối hợp, hỗ trợ và tạo điều kiện thuận lợi để thực hiện công tác ứng cứu, xử lý sự cố.

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

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

- Nội dung thực hiện: 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 chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

2.3. Xử lý sự cố, gỡ bỏ và khôi phục

a) Xử lý sự cố, gỡ bỏ:

- Nội dung thực hiện: Sau khi đã triển khai ngăn chặn sự cố, đơn vị sử dụng, quản lý, vận hành hệ thống thông tin, cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng triển khai biện pháp 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.

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

b) Khôi phục:

- Nội dung thực hiện: Đơn vị sử dụng, 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 cho hệ thống thông tin.

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

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

- Nội dung thực hiện: Đơn vị sử dụng, quản lý, vận hành hệ thống thông tin và các cơ quan, 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 hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ

chức các bước tương ứng tại Khoản 2.2 và Khoản 2.3 của Kế hoạch này để khôi phục hoạt động bình thường của hệ thống thông tin.

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

2.4. Tổng kết, đánh giá

- Nội dung thực hiện: Phòng TCHC tổng hợp báo cáo sự cố, công tác triển khai phương án ứng cứu sự cố, báo cáo chủ quản hệ thống thông tin, 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; 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.

- Đơn vị chủ trì thực hiện: Cán bộ phụ trách công nghệ thông tin và Phòng TCHC.

- Đơn vị phối hợp: Các phòng chuyên môn.

III. TỔ CHỨC THỰC HIỆN

1. Trên cơ sở Kế hoạch này, các phòng: Tổ chức hành chính; QLDA 1; QLDA 2; QLDA 3; Môi trường xã hội; Tài chính kế toán triển khai thực hiện.

2. Giao Phòng Tổ chức hành chính và cán bộ phụ trách công nghệ thông tin chủ trì, phối hợp với các bộ phận chuyên môn trao đổi thông tin, xử lý những vấn đề có liên quan đến việc ứng phó sự cố, bảo đảm an toàn thông tin mạng của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa.

3. Giao Phòng Tổ chức hành chính chủ trì, phối hợp với phòng Tài chính kế toán bố trí kinh phí để ứng phó sự cố, bảo đảm an toàn thông tin mạng của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa năm 2019.

4. Trong quá trình triển khai thực hiện Kế hoạch này, nếu có khó khăn vướng mắc, đề nghị các phòng có ý kiến phản hồi để phòng TCHC tổng hợp báo cáo lãnh đạo Ban xem xét, quyết định.

Trên đây là Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng của Ban Quản lý dự án Phát triển tỉnh Khánh Hòa năm 2019./.

***Nơi nhận*:**
- Sở Thông tin & Truyền thông (VBĐT, b/c);
- Các phòng chuyên môn của Ban (VBĐT);
- Trang Web của Ban;
- Lưu VT, TCHC.

GIÁM ĐỐC

BAN QUẢN LÝ DỰ ÁN PHÁT TRIỂN TỈNH KHÁNH HÒA

Châu Ngô Anh Nhân