UBND TỈNH KHÁNH HÒA
BAN QLDA ĐẦU TƯ XÂY DỰNG CÁC CÔNG TRÌNH NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN

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

Số: 166 /KH-BQLNN

Khánh Hòa, ngày 24 tháng 3 năm 2021

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng của Ban quản lý dự án đầu tư xây dựng các công trình Nông nghiệp và Phát triển nông thôn tỉnh Khánh Hòa năm 2021

Căn cứ Kế hoạch số 1312/KH-UBND ngày 23/02/2021 của UBND tỉnh Khánh Hòa về việc ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2021;

Ban quản lý dự án đầu tư xây dựng các công trình Nông nghiệp và Phát triển nông thôn tỉnh Khánh Hòa xây dựng và triển khai Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng của Ban năm 2021, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Nhằm đảm bảo an toàn thông tin cho hệ thống thông tin quan trọng của Ban, đảm bảo khả năng có thể xử lý 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 và hướng khắc phục khi gặp sự cố mất an toàn thông tin mạng.

- Tuyên truyền, phổ biến mức độ rủi ro về sự cố mất an toàn thông tin mạng để nâng cao nhận thức về an toàn thông tin đối với cán bộ công chức, viên chức và người lao động trong cơ quan.

- 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

- Căn cứ trên kết quả khảo sát, đánh giá các nguy cơ, sự cố mất an toàn thông tin mạng trên hệ thống thông tin của các cơ quan Nhà nước trên địa bàn tỉnh và trên cơ sở đó đối chiếu với tình hình thực tế của Ban trong thời gian qua, để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời và phù hợp.

- Có phương án 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 của sự cố khi sự cố xảy ra.

- Đảm bảo nguồn lực, 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 đến toàn thể công chức, viên chức và người lao động trong Ban về các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng, nội dung thực hiện:

- Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính Phủ về việc 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.

- 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.

2. Phối hợp tham gia triển khai các phương án, chương trình huấn luyện, diễn tập

- Nội dung thực hiện: Phối hợp tham gia tập huấn, 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, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố.

- Thời gian thực hiện: Theo kế hoạch của cơ quan chuyên trách ứng cứ sự cố an toàn thông tin mạng của tỉnh (Sở Thông tin và Truyền thông).

3. Triển khai hướng dẫn phương án phòng ngừa sự cố, giám sát phát hiện sớm sự cố

- Nội dung thực hiện: Cập nhật thông tin từ Trung tâm giám sát an toàn không gian mạng quốc gia, Sở thông tin và Truyền thông và Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cử cán bộ tham gia các khóa đào tạo, bồi dưỡng kỷ năng giám sát, đánh giá 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.

- Thời gian thực hiện: Định kỳ hàng quý.

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, 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.

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

- Nội dung thực hiện: Triển khai các phương án, hướng dẫn phòng ngừa sự cố; thực hiện việc kiểm tra, đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của hệ thống thông tin; dự báo các nguy cơ, sự cố tấn công mạng có thể xảy ra với hệ thống thông tin; 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.

6. 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

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 như:

- 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…

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; lấy cắp thông tin, dữ liệu; tấn công tổng hợp sử dụng kết hợp nhiều hình thức và 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) Phối hợp với Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa để ngăn chặn, khắc phục sự cố.

d) Lập 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.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện theo dự toán chi phí Ban 2021.

IV. TỔ CHỨC THỰC HIỆN

- Phòng Tài chính - Tổng hợp chủ trì, phối hợp với các Phòng nghiệp vụ và cán bộ phụ trách công nghệ thông tin tham mưu Lãnh đạo Ban triển khai thực hiện Kế hoạch này, phối hợp xử lý những vấn đề có liên quan đến việc ứng dụng công nghệ thông tin và bảo đảm an toàn thông tin mạng trong hoạt động của Ban được hiệu quả.

- Trong quá trình tổ chức thực hiện kế hoạch này, nếu có khó khăn vướng mắc, đề nghị các Phòng đóng góp ý kiến qua phòng Tài chính - Tổng hợp để tổng hợp báo cáo Lãnh đạo Ban xem xét, quyết định.

- Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, đề nghị các Phòng nghiệp vụ, cán bộ CCVC có ý kiến góp ý gửi Phòng Tài chính – Tổng hợp để tổng hợp trình Lãnh đạo Ban xem xét, sửa đổi và điều chỉnh cho phù hợp./.

Nơi nhận:
- Sở TTTT KH *(để biết)*; VBĐT
- Các Phòng nghiệp vụ; (VBĐT)
- Lưu:VT, A.Phong.

GIÁM ĐỐC

Quách Thanh Sơn