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: 199 /KH-BQLNN

Khánh Hòa, ngày 13 tháng 4 năm 2023

KẾ HOẠCH
Ứng phó sự cố và bảo đảm an toàn thông tin mạng năm 2023

Triển khai thực hiện Kế hoạch số 2517/KH-UBND ngày 17/3/2022 của UBND tỉnh Khánh Hòa về Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2023; Kế hoạch số 244/KH-BQLNN ngày 24/5/2022 của Ban QLDA đầu tư xây dựng các công trình Nông nghiệp và Phát triển nông thôn về Ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước và phát triển chính quyền số giai đoạn 2022 – 2025.

Căn cứ nhiệm vụ chuyên môn được giao, Ban Quản lý dự án đầu tư xây dựng các công trình Nông nghiệp và Phát triển nông thôn xây dựng Kế hoạch Ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2023 với những nội dung cụ thể sau đây:

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 cho cán bộ, viên chức trong cơ quan.

- Đảm bảo nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai ứng phó kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố bảo đảm an toàn thông tin mạng và phối hợp với các cơ quan chuyên môn để ngăn chặn, khắc phục...

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. Trên cơ sở đó kiểm tra, rà soát, đối chiếu với tình hình thực tế của Ban 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 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.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác bảo đảm an toàn thông tin giữa các cơ quan nhà nước trên địa bàn tỉnh và sự hỗ trợ của Sở Thông tin và Truyền thông.

II. NHIỆM VỤ TRIỂN KHAI

1. Tuyên truyền, phổ biến đến toàn thể cán bộ, 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 tuyên truyền, phổ biến: 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; 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...; 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.

- Thời gian thực hiện: Thường xuyên trong năm, đăng tải trên Trang thông tin điện tử của Ban.

2. Tham gia triển khai các phương án, chương trình huấn luyện, diễn tập

- Nội dung thực hiện: Cử cán bộ chuyên trách CNTT 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 do các cơ quan chuyên môn, Sở Thông tin và Truyền thông tổ chức nhằm 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 (SOC), Sở Thông tin và Truyền thông và Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Kiểm tra, rà soát phát hiện sớm các nguy cơ, sự cố, đánh giá mức độ mất an toàn thông tin mạng; rà quét, bóc gỡ, phân tích, xử lý mã độc; 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 cho cán bộ, viên chức; thường xuyên trao đổi phối hợp với Trung tâm dự liệu tỉnh kiểm tra vấn đề nâng cấp giao thức bảo mật cho các Trang thông tin điện tử của Ban.

- Thời gian thực hiện: Thường xuyên trong năm.

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.

- Thời gian thực hiện: Thường xuyên trong năm

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) Tiếp nhận, phân tích, thông báo sự cố nhanh chóng, kịp thời và ứng cứu ban đầu.

- Sự cố do bị tấn công mạng từ các nguồn bên trong và bên ngoài. Xác minh sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố.

- 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) Triển khai ứng cứu, ngăn chặn và xử lý sự cố:

Phân tích, xác định phạm vi ảnh hưởng, 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.

c) Xử lý sự cố, gỡ bỏ, khôi phục và xử lý vi phạm

- Tình huống sự cố do bị tấn công mạng: Triển khai ngăn chặn sự cố, đồng thời tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu mất an toàn thông tin của hệ thống thông tin. Liên hệ, phối hợp với Sở Thông tin Truyền thông và Đội Ứng khẩn cấp sự cố an toàn thông tin mạng tỉnh để có hướng ngăn chặn, khắc phục sự cố.

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

d) Tổng hợp báo cáo, đánh giá.

Cán bộ phụ trách CNTT phối hợp với các phòng nghiệp vụ tổng hợp báo cáo, phân tích sự cố, công tác triển khai phương án ứng cứu sự cố cho Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa và Sở Thông tin và Truyền thông và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai.

III. KINH PHÍ THỰC HIỆN

Ban Quản lý dự án đầu tư xây dựng các công trình Nông nghiệp và Phát triển nông thôn tỉnh Khánh Hòa là đơn vị sự nghiệp công lập tự đảm bảo chi thường xuyên về tài chính. Do vậy, kinh phí thực hiện được trích từ nguồn kinh phí hoạt động thường xuyên của cơ quan.

IV. TỔ CHỨC THỰC HIỆN

1. 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 liên quan đến việc ứng phó sự cố, bảo đảm an toàn thông tin mạng khi có phát hiện sự cố trong cơ quan.

- 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.

2. Ban biên tập Trang thông tin điện tử: Thường xuyên theo dõi, đăng tải, cập nhật đầy đủ các thông tin trên Trang thông tin điện tử.

3. Ban QLDA đầu tư xây dựng các công trình Nông nghiệp và Phát triển nông thôn đề nghị Trưởng các phòng: Tài chính-Tổng hợp, Quản lý dự án, Giải phóng mặt bằng và toàn thể cán bộ, viên chức quán triệt, thực hiện có chất lượng, hiệu quả nội dung Kế hoạch này./.

Nơi nhận:
- Sở Thông tin và Truyền thông; *(VBĐT)*
- Phòng TCTH, QLDA, GPMB;
- Trang TTĐT;
- Lưu VT.

GIÁM ĐỐC

BAN QUẢN LÝ DỰ ÁN ĐẦU TƯ XÂY DỰNG CÁC CÔNG TRÌNH NÔNG NGHIỆP VÀ PHÁT TRIỂN NÔNG THÔN TỈNH KHÁNH HÒA

Quách Thanh Sơn