UBND TỈNH KHÁNH HÒA
BAN QUẢN LÝ KHU KINH TẾ VÂN PHONG

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

Số: 2923 /KH-KKT

Khánh Hòa, ngày 12 tháng 12 năm 2024

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2024 của Ban quản lý Khu kinh tế Vân Phong

Thực hiện Kế hoạch số 12830/KH-UBND ngày 04/12/2023 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 2024;

Ban quản lý Khu kinh tế Vân Phong (Ban quản lý) xây dựng Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2024, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU:

1. Mục đích:

- Đảm bảo an toàn thông tin mạng cho các hệ thống thông tin của Ban quản lý; 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 nhằm 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 hệ thống thông tin của Ban quản lý.

- Nâng cao nhận thức về an toàn thông tin trên hệ thống mạng cho đội ngũ công chức, viên chức và người lao động (CCVC) của Ban quản lý.

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

2. Yêu cầu:

- 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; đồng thời 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.

- 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.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác đảm bảo an toàn thông tin giữa các cơ quan nhà nước trên địa bàn tỉnh; phối hợp, hỗ trợ với các đơn vị liên quan.

II. NHIỆM VỤ TRIỂN KHAI:

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

- Tổ chức tuyên truyền, phổ biến, hướng dẫn các nội dụng của Luật An toàn thông tin mạng; 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 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 và 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; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của 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; Chỉ thị 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 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ về tăng cường công tác đảm bảo an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát; các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng trên phần mềm quản lý văn bản và trên trang thông tin điện tử của Ban quản lý.

- Cử CCVC tham gia các lớp tập huấn về ứng phó sự cố, đảm bảo an toàn thông tin mạng.

- Đảm bảo 100% máy tính CCVC cài đặt phần mềm diệt virus, thường xuyên cập nhật cơ sở dữ liệu mới và kết nối với máy chủ giám sát an toàn thông tin của tỉnh.

- Thường xuyên theo dõi, giám sát các hệ thống thông tin nội bộ của Ban quản lý, kịp thời phát hiện sự cố mất an toàn và cập nhật các bản vá lỗi cho hệ thống.

- Tổ chức khảo sát, kiểm tra hệ thống, giám sát định kỳ và có phương án nâng cấp, sửa chữa hệ thống nhằm đảm bảo hệ thống hoạt động ổn định, hiệu quả.

- 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.

- Xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng đối với mỗi hệ thống thông tin, chương trình, ứng dụng.

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

- Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố: thường xuyên theo dõi, tiếp nhận, phân tích cảnh báo, dấu hiệu sự cố, xác minh sự cố xảy ra và thông báo đến các cơ quan liên quan.

- Triển khai ứng cứu, ngăn chặn và xử lý sự cố: triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng; phân tích, xác định nguồn tấn

công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

- Xử lý sự cố, gỡ bỏ và khôi phục: sau khi ngăn chặn sự cố, tiến hành gỡ bỏ mã độc, khắc phục điểm yếu an toàn thông tin của hệ thống, khôi phục lại hệ thống thông tin và đánh giá lại hệ thống.

- Tổng kết, đánh giá:

+ Tiến hành tổng hợp toàn bộ các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ứng cứu sự cố và báo cáo với cơ quan liên quan.

+ Tổ chức đánh giá lại, 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.

III. KINH PHÍ THỰC HIỆN:

Kinh phí thực hiện Kế hoạch này được sử dụng từ nguồn kinh phí phục vụ nhiệm vụ chuyển đổi số.

IV. TỔ CHỨC THỰC HIỆN:

1. Văn phòng:

- Chủ trì tổ chức thực hiện các nhiệm vụ theo Mục II Kế hoạch này.

- Thường trực tiếp nhận, phối hợp xử lý và báo cáo sự cố ngay sau khi tiếp nhận sự cố.

- Theo dõi, kiểm tra và đôn đốc CCVC cơ quan thực hiện tốt các nội dung nhằm giảm thiểu tối đa ảnh hưởng khi gặp phải sự cố.

- Xây dựng dự toán kinh phí hàng năm và giai đoạn cho hoạt động ứng cứu sự cố, bảo đảm an toàn thông tin mạng của Ban quản lý.

2. Các phòng, đơn vị:

- Chịu trách nhiệm phối hợp với Văn phòng kiểm tra và đôn đốc CCVC của phòng thực hiện các nội dung liên quan theo kế hoạch.

Trong quá trình triển khai thực hiện, nếu có vướng mắc, bất cập, các phòng, đơn vị trực thuộc đề xuất Văn phòng tổng hợp báo cáo Lãnh đạo Ban kịp thời xử lý./.

Nơi nhận:
- UBND tỉnh -b/c (VBĐT);
- Sở TTTT (VBĐT);
- LĐ Ban (VBĐT);
- Các phòng, BQLDA (VBĐT);
- Lưu: VT, VP, VTĐ, 02.

KT. TRƯỞNG BAN
PHÓ TRƯỞNG BAN

BAN QUẢN LÝ KHU KINH TẾ VĂN PHONG KHÁNH HÒA

Vương Thị Lệ Huyền