

Số: /KH-UBND

Đại Lãnh, ngày tháng 01 năm 2024

KẾ HOẠCH

Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn xã Đại Lãnh năm 2024

Thực hiện Kế hoạch số 12/KH-UBND ngày 03/01/2024 của UBND huyện Vạn Ninh về ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn huyện Vạn Ninh năm 2024;

UBND xã Đại Lãnh xây dựng kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn xã Đại Lãnh năm 2024 với các nội dung như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng trên địa bàn xã; bảo đảm 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.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với lực lượng công chức.

- Bảo đảm 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 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 của hệ thống thông tin của huyện để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp.

- 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.

- Xác định cụ thể các nguồn lực, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, bảo đảm 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; tận dụng sự phối hợp, hỗ trợ của các đơn vị nghiệp vụ của Bộ Thông tin và Truyền thông và Sở Thông tin và Truyền thông tỉnh Khánh Hòa.

II. NHIỆM VỤ TRIỂN KHAI

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

1.1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng

- Nội dung thực hiện: Tổ chức tuyên truyền, phổ biến, hướng dẫn nội dung của 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; 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; Chỉ thị số 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 số 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát; 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 và các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng trên các phương tiện thông tin đại chúng, Trang TTĐT của xã.

- Đơn vị thực hiện: Cán bộ Văn hóa và Thông tin.
- Đơn vị phối hợp: Ban Biên tập Trang TTĐT xã; các công chức chuyên môn.
- Thời gian thực hiện: Thực hiện thường xuyên trong năm.

1.2. Triển khai các chương trình đào tạo, bồi dưỡng kỹ năng đánh giá, ứng phó sự cố

- Nội dung thực hiện: Tham gia các lớp 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; 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, đào tạo, bồi dưỡng, diễn tập vùng, miền, quốc gia, quốc tế theo triệu tập của cơ quan chuyên môn.

- Đơn vị thực hiện: thành viên Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.
- Đơn vị phối hợp: Công chức Văn phòng – Thống kê; Cán bộ Văn hóa và Thông tin và các công chức chuyên môn.
- Thời gian thực hiện: trong năm 2024.

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

- Nội dung thực hiện:
 - + Triển khai thực hiện hệ thống Trung tâm Giám sát an toàn thông tin mạng

(SOC), kết nối Trung tâm Giám sát an toàn không gian mạng quốc gia, mở rộng phạm vi giám sát đến các ban ngành chuyên môn xã; tổ chức 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, xác minh, cảnh báo sự cố, rủi ro an toàn thông tin mạng, phân 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.

+ Rà soát đánh giá tình hình, công tác phòng ngừa sự cố trong thời gian qua, xác định những mặt trọng tâm, trọng điểm có nguy cơ, từ đó tập trung triển khai các biện pháp bảo vệ, phòng ngừa; chú ý sắp xếp, bố trí cán bộ đủ năng lực chuyên môn, có phẩm chất tốt để đảm nhiệm những vị trí quan trọng trong quản lý, vận hành các hệ thống thông tin. Chú trọng vấn đề nâng cấp giao thức bảo mật cho Trang thông tin điện tử, cơ sở hạ tầng mạng trong hệ thống thông tin của địa phương.

- Đơn vị thực hiện: Công chức Văn phòng – Thống kê; Cán bộ Văn hóa và Thông tin; thành viên Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Công an xã; các công chức chuyên môn.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); Trung tâm Giám sát an toàn không gian mạng quốc gia; Sở Thông tin và Truyền thông tỉnh Khánh Hòa; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh và các đơn vị liên quan khác.

- Thời gian thực hiện: Thường xuyên trong năm.

1.4. 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 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; 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 thực hiện: Công chức Văn phòng – Thống kê; Cán bộ Văn hóa và Thông tin; thành viên Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Công an xã; các công chức chuyên môn.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); Trung tâm Giám sát an toàn không gian mạng quốc gia; Sở Thông tin và Truyền thông tỉnh Khánh Hòa; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh và các đơn vị liên quan khác.

- Thời gian thực hiện: Thường xuyên trong năm.

1.5. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

- Nội dung thực hiện: Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng đối với hệ thống thông tin; đánh giá, dự báo các nguy cơ, sự cố hệ thống thông tin có thể xảy ra; dự báo đối tượng có thể tấn công, phá hoại

gây ra sự cô mất an toàn thông tin mạng; 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 phục vụ đối phó, ứng cứu, khắc phục sự cố của địa phương (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

- Đơn vị thực hiện: Công chức Văn phòng – Thống kê; Cán bộ Văn hóa và Thông tin; thành viên Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Công an xã; các công chức chuyên môn.

- Đơn vị phối hợp: Phòng Văn hóa – Thông tin, Sở Thông tin và Truyền thông; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh; các nhà thầu cung cấp dịch vụ an toàn thông tin mạng (nếu có); các đơn vị khác liên quan.

- Thời gian thực hiện: Cơ quan chủ quản hệ thống thông tin tự chủ trì đánh giá, kiểm tra hệ thống thông tin định kỳ 06 tháng (trước ngày 10/6), 01 năm (trước ngày 05/12).

1.6. Xây dựng phương án đối phó, ứng cứu đối với một số tình huống sự cố về an toàn thông tin mạng, cụ thể

- An toàn thông tin mạng

- Triển khai các nhiệm vụ tại Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng năm 2024; Nâng cấp hệ thống an toàn thông tin mạng, ứng phó sự cố mạng UBND xã Đại Lãnh; kế hoạch triển khai Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ CNTT; Kế hoạch triển khai Đề án “Tuyên truyền, nâng cao, nhận thức và phổ biến kiến thức về an toàn thông tin giai đoạn 2021-2025”; Kế hoạch đào tạo và phát triển nguồn nhân lực an toàn thông tin giai đoạn 2021-2025 trên địa bàn tỉnh Khánh Hòa theo lộ trình.

+ Tăng cường năng lực hạ tầng kỹ thuật, năng lực giám sát ATTT cho UBND xã phục vụ triển khai chuyển đổi số, phát triển Chính quyền số xã. Khi đầu tư, mua sắm, thuê dịch vụ về trang thiết bị, giải pháp kỹ thuật, nhân lực vận hành an toàn thông tin, cần triển khai đầy đủ các nhiệm vụ bảo đảm an toàn thông tin mạng như Phần mềm nội bộ do đơn vị chuyên nghiệp phát triển, tuân thủ theo quy trình Khung phát triển phần mềm an toàn tại Công văn số 166/BTTTT-ATHTTT ngày 10/2/2022 của Bộ Thông tin và Truyền thông; hệ thống thông tin triển khai đầy đủ phương án bảo đảm an toàn thông tin theo cấp độ và phải được kiểm tra, đánh giá an toàn thông tin mạng trước khi đưa vào sử dụng, khi nâng cấp, thay đổi, định kỳ theo quy định; hệ thống thông tin được quản lý, vận hành theo mô hình 4 lớp theo Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ.

- Phương án đối phó, ứng cứu sự cố an toàn thông tin mạng

Đối với mỗi hệ thống thông tin và 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 cơ quan quản lý, vận hành hệ thống thông tin, chương trình ứng dụng phải xây dựng phương án đối phó, ứng cứu sự cố theo hướng dẫn của Sở

Thông tin và Truyền thông và các đơn vị chuyên môn thuộc Bộ Thông tin và Truyền thông.

- Đơn vị thực hiện: Công chức Văn phòng – Thống kê; Cán bộ Văn hóa và Thông tin; thành viên Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Công an xã; các công chức chuyên môn.

- Đơn vị phối hợp: Phòng Văn hóa – Thông tin huyện; Sở Thông tin và Truyền thông; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh; cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); các đơn vị khác liên quan.

- Thời gian thực hiện: Sau khi Kế hoạch ứng phó sự cố được UBND xã ban hành.

2. Triển khai các nhiệm vụ khi có sự cố xảy ra: thực hiện theo *Quy trình ứng cứu, xử lý khẩn cấp sự cố tấn công mạng* tại Phụ lục ban hành kèm theo Kế hoạch số 12830/KH-UBND ngày 04/12/2023 của UBND tỉnh Khánh Hòa đính kèm theo Kế hoạch này.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch này được bố trí từ nguồn ngân sách hàng năm của địa phương.

IV. TỔ CHỨC THỰC HIỆN

1. Các công chức chuyên môn, Công an xã

- Các công chức chuyên môn, Trưởng Công an xã căn cứ nội dung Kế hoạch này và tình hình thực tế tại địa phương căn cứ thực hiện Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng của đơn vị, bảo đảm đúng tiến độ, chất lượng, hiệu quả và tiết kiệm, tránh hình thức, lãng phí.

- Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch chuyển đổi số và bảo đảm an toàn thông tin mạng hàng năm của cơ quan, đơn vị để triển khai các nhiệm vụ được giao tại Kế hoạch này hoặc chủ động xây dựng dự toán kinh phí chi tiết, gửi về Công chức Tài chính – Kế toán tổng hợp, trình UBND xã phê duyệt, cấp kinh phí thực hiện các nhiệm vụ.

- Phân công lãnh đạo phụ trách an toàn thông tin, chỉ định bộ phận đầu mối chịu trách nhiệm về an toàn thông tin mạng của cơ quan.

- Thực hiện bố trí cán bộ, công chức chuyên trách về an toàn thông tin mạng tại địa phương mình.

- Cử cán bộ tham gia các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn bảo đảm an toàn thông tin mạng để nâng cao kỹ năng và công tác tham mưu triển khai giám sát, bảo đảm an toàn thông tin.

2. Công chức Văn phòng – Thống kê phụ trách CNTT

- Chủ trì, phối hợp Công chức Văn hoá và xã hội xử lý sự cố máy tính, mạng đường truyền số liệu chuyên dùng của huyện; rà soát hệ thống máy tính và trang thông tin điện tử nhằm phát hiện, xây dựng các giải pháp khắc phục điểm yếu có

nguy cơ gây mất an ninh thông tin; triển khai các phương án phòng ngừa sự cố, giám sát phát hiện sớm các sự cố; kiểm tra đánh giá an toàn thông tin mạng và rà quét, bóc gỡ, phân tích xử lý mã độc.

- 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 và hướng dẫn tại 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 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ theo quy định.

- Khẩn trương thực hiện việc xác định cấp độ và xây dựng hồ sơ đề xuất cấp độ an toàn thông tin đối với hệ thống thông tin có sử dụng camera giám sát theo Chỉ thị số 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát, gửi về Phòng Văn hóa – Thông tin tổng hợp gửi Sở Thông tin và Truyền thông Thẩm định.

- Cử chuyên viên Quản trị mạng xã tham gia Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa và kịp thời thông báo về Sở Thông tin và Truyền thông khi có sự thay đổi cán bộ, công chức chuyên trách về an toàn thông tin mạng.

- Cử cán bộ tham gia các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn bảo đảm an toàn thông tin mạng để nâng cao kỹ năng và công tác tham mưu triển khai giám sát, bảo đảm an toàn thông tin.

3. Công chức Văn hóa và Xã hội: hướng dẫn các ngành, đoàn thể trên địa bàn xã tuyên truyền những quy định về đảm bảo an toàn, an ninh hệ thống thông tin. Tham mưu UBND xã cử cán bộ, công chức tham gia các lớp tập huấn về kiến thức an ninh, an toàn thông tin cho lãnh đạo UBND và cán bộ, công chức nhằm thực hiện an ninh, an toàn thông tin; tăng cường công tác quản lý nhà nước đối với các hoạt động sử dụng dịch vụ internet, dịch vụ bưu chính viễn thông nhằm kịp thời ngăn chặn phát hiện và xử lý các tổ chức, cá nhân có hành vi vi phạm an toàn, an ninh thông tin trên địa bàn huyện; phối hợp Công chức Văn phòng – Thống kê 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 và hướng dẫn tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông theo quy định và xử lý sự cố máy tính, mạng đường truyền số liệu chuyên dùng của xã, rà soát hệ thống máy tính và trang thông tin điện tử nhằm phát hiện, xây dựng các giải pháp khắc phục điểm yếu có nguy cơ gây mất an ninh thông tin.

4. Công chức Tài chính – Kế toán: trên cơ sở dự toán của địa phương, Công chức Tài chính - Kế toán cân đối ngân sách, tham mưu cấp có thẩm quyền xem xét, bố trí kinh phí thực hiện Kế hoạch này.

5. Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các ban ngành, đoàn thể, cán bộ, công chức kịp thời phối hợp với Công chức Văn hoá và

Xã hội, cán bộ phụ trách CNTT để tổng hợp, báo cáo UBND xã xem xét, giải quyết theo thẩm quyền.

Trên đây là Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn xã Đại Lãnh năm 2024.

(Đính kèm phụ lục Quy trình ứng cứu, xử lý khẩn cấp sự cố tấn công mạng)./.

Nơi nhận:

- UBND huyện (để b/c);
- Phòng VH TT (để b/c);
- TT Đảng ủy (để b/c);
- CT và các PCT UBND xã (để b/c);
- Mặt trận và các đoàn thể (để T/H);
- Các ban ngành liên quan (để T/H);
- Trang Thông tin điện tử xã;
- Lưu: VT, VP, T15.

**TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**

Trần Duy Khoang