

Số: /KH-UBND

Ea Kar, ngày tháng 01 năm 2026

KẾ HOẠCH

Ứng phó sự cố, bảo đảm an toàn, an ninh thông tin mạng trong hoạt động của UBND xã Ea Kar năm 2026

I. CĂN CỨ XÂY DỰNG KẾ HOẠCH

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ quy định về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ 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;

Căn cứ 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;

Căn cứ Quyết định số 05/2017/QĐTTg 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;

Căn cứ 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;

Căn cứ 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;

Để tăng cường công tác bảo đảm an ninh mạng, an toàn thông tin mạng theo quy định. UBND xã Ea Kar ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn, an ninh thông tin mạng trong hoạt động cơ quan năm 2026, như sau:

II. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Đảm bảo an toàn thông tin mạng cho hệ thống thông tin của cơ quan; 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 kịp thời 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 UBND xã.

- Nâng cao nhận thức về an toàn thông tin trên hệ thống mạng cho đội ngũ cán bộ, công chức và người lao động trong các cơ quan, đơn vị.

- Đảm bảo các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng phó khi có sự cố 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, đơn vị; sự hỗ trợ của các đơn vị liên quan cấp trên.

III. NỘI DUNG 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 dung của Luật An toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Quyết định số 05/2017/QĐTTg ngày 16/3/2017 của Thủ tướng Chính phủ; Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông; Chỉ thị 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ; Chỉ thị 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ; các văn bản có liên quan khác về an toàn thông tin mạng.

Cử công chức, viên chức tham gia các lớp tập huấn về ứng phó sự cố, đảm bảo an toàn thông tin mạng khi các sở, ngành tổ chức.

Thường xuyên theo dõi, giám sát các hệ thống thông tin nội bộ của cơ quan, 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.

Thời gian thực hiện: Thường xuyên trong năm, các cơ quan, đơn vị.

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

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.

Tổng kết, đánh giá khi có dấu hiệu sự cố hoặc sự cố xảy ra:

- 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 để tìm nguyên nhân.

- 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.

IV. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch này được sử dụng từ nguồn ngân sách nhà nước, bố trí cho thực hiện nhiệm vụ chuyển đổi số, theo Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ trưởng Bộ Tài chính quy định về lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện công tác ứng cứu sự cố, đảm bảo an toàn thông tin.

V. TỔ CHỨC THỰC HIỆN

1. Công an xã:

Chủ trì, hướng dẫn các phòng chuyên môn, các trung tâm, các cơ quan đơn vị trực thuộc xã thực hiện đảm bảo an toàn, an ninh thông tin mạng. Kịp thời phát hiện, đề xuất xử lý các trường hợp cung cấp thông tin sai lệch, không đúng sự thật trên không gian mạng.

2. Phòng Văn hóa - Xã hội:

- Chủ trì, phối hợp các cơ quan, đơn vị liên quan tổ chức thực hiện các nhiệm vụ của Kế hoạch này đảm bảo an ninh mạng, an toàn thông tin mạng theo quy định. Thường trực tiếp nhận, phối hợp xử lý và báo cáo sự cố ngay sau khi tiếp nhận sự cố về an toàn thông tin mạng.

- Thường xuyên theo dõi, đôn đốc các cơ quan, đơn vị thực hiện các nhiệm vụ của Kế hoạch, kịp thời báo cáo UBND xã và cơ quan cấp trên xử lý, tháo gỡ khó khăn trong quá trình triển khai.

- Chủ động phối hợp Sở Khoa học và Công nghệ, cập nhật thông tin tuyên truyền mới, để triển khai phổ biến đến cán bộ, công chức, viên chức và người lao động về an ninh, an toàn thông tin mạng.

- Phối hợp các phòng chuyên môn đề xuất nhu cầu, kinh phí để duy trì thực hiện Hệ thống Giám sát an toàn thông tin tại trụ sở UBND xã đảm bảo hệ thống hoạt động thông suốt, cảnh báo kịp thời các sự cố về thông tin mạng; phòng chống mã độc và diệt vi rút theo quy định.

3. Phòng Kinh tế:

Chủ trì, tham mưu UBND xã bố trí kinh phí đảm bảo cho hoạt động bảo đảm an ninh mạng, an toàn thông tin mạng trên địa bàn xã. Hướng dẫn các thủ tục liên quan đến hoạt động mua sắm, trang bị các thiết bị, dụng cụ cần thiết và thanh quyết toán theo quy định.

4. Văn phòng HĐND&UBND, Trung tâm Phục vụ hành chính công; Trung tâm Cung ứng Dịch vụ sự nghiệp công

Triển khai thực hiện Kế hoạch này, đảm bảo thực hiện nhiệm vụ an toàn thông tin mạng trong phạm vi, nhiệm vụ của cơ quan, đơn vị. Rà soát, đề xuất nhu cầu, kinh phí để thực hiện đảm bảo an toàn thông tin mạng; phòng chống mã độc, nội dung đề xuất gửi về UBND xã để xem xét bố trí theo quy định.

Trên đây là Kế hoạch ứng phó sự cố, bảo đảm an toàn, an ninh thông tin mạng trong hoạt động của UBND xã Ea Kar. Trong quá trình triển khai thực hiện, nếu có vướng mắc, bất cập, các bộ phận kịp thời báo cáo Lãnh đạo UBND xã để kịp thời xem xét, điều chỉnh, bổ sung cho phù hợp./.

Nơi nhận:

- Chủ tịch, các Phó CT UBND xã;
- Các phòng chuyên môn xã;
- Trung tâm Cung ứng DVSNC xã;
- Trung tâm PVHCC xã;
- Lưu: VT.

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**

Nguyễn Thanh Dương