ỦY BAN NHÂN DÂN **XÃ CẨM XUYÊN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh phúc**
Số: 3514 /KH-UBND	*Cẩm Xuyên, ngày 31 tháng 10 năm 2026*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng tại UBND xã Cẩm Xuyên

Căn cứ Luật Công nghệ thông tin ngày 29/6/2006; Luật An toàn thông tin mạng ngày 19/11/2015; Luật An ninh mạng ngày 12/6/2018;

Căn cứ 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;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

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;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ 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;

Căn cứ Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng;

Căn cứ Kế hoạch số 150/KH-UCSCATTTM ngày 08/5/2026 của Đội Ứng cứu sự cố An toàn thông tin mạng về việc Kế hoạch hoạt động đội ứng cứu sự cố an toàn thông tin mạng tỉnh Hà Tĩnh năm 2026;

UBND xã Cẩm Xuyên ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng tại UBND xã Cẩm Xuyên như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin cho các hệ thống thông tin, cơ sở dữ liệu, trang thiết bị công nghệ thông tin của UBND xã Cẩm Xuyên.
- Chủ động phòng ngừa, phát hiện sớm và kịp thời xử lý các nguy cơ mất an toàn thông tin, tấn công mạng, lây nhiễm mã độc.
- Nâng cao nhận thức, trách nhiệm của cán bộ, công chức, người lao động trong công tác bảo đảm an toàn thông tin mạng.

2. Yêu cầu

- Xây dựng lực lượng ứng cứu sự cố an toàn thông tin mạng của xã đáp ứng yêu cầu nhiệm vụ trong tình hình mới.

- Bảo đảm duy trì hoạt động thông suốt của hệ thống thông tin phục vụ chỉ đạo điều hành, giải quyết thủ tục hành chính và chuyển đổi số tại UBND xã.

- Các hệ thống thông tin của xã phải được rà soát, đánh giá nguy cơ mất an toàn thông tin định kỳ.

- Công tác ứng cứu sự cố phải được triển khai kịp thời, đúng quy trình, hạn chế thấp nhất thiệt hại.

- Tăng cường phối hợp giữa các bộ phận chuyên môn, Công an xã, các doanh nghiệp viễn thông và cơ quan chuyên trách cấp trên.

- Bảo đảm đầy đủ nhân lực, trang thiết bị, kinh phí phục vụ công tác ứng cứu sự cố.

II. PHẠM VI VÀ ĐỐI TƯỢNG ÁP DỤNG, NGUYÊN TẮC ỨNG PHÓ

1. Phạm vi

- Kế hoạch này áp dụng đối với các hệ thống thông tin, thiết bị công nghệ thông tin, hệ thống mạng nội bộ, hệ thống thư điện tử công vụ, trang thông tin điện tử và các nền tảng số thuộc phạm vi quản lý của UBND xã Cẩm Xuyên.

2. Đối tượng áp dụng

- Các phòng, ban, đơn vị chuyên môn thuộc UBND xã;

- Công an xã;

- Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet và dịch vụ công nghệ thông tin có liên quan.

- Toàn thể cán bộ, công chức, viên chức, người lao động.

3. Nguyên tắc ứng phó sự cố

- Chủ động phòng ngừa, phát hiện sớm, xử lý kịp thời.

- Thực hiện theo phương châm "4 tại chỗ".

- Bảo đảm phối hợp chặt chẽ giữa các lực lượng tham gia ứng cứu.

- Bảo đảm bí mật thông tin trong quá trình xử lý sự cố.

- Ưu tiên duy trì hoạt động của các hệ thống thông tin phục vụ chỉ đạo điều hành và giải quyết thủ tục hành chính.

III. NỘI DUNG THỰC HIỆN

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

- Nội dung thực hiện:

+ Thường xuyên rà soát, đánh giá hiện trạng bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin, phần mềm ứng dụng, trang thiết bị công nghệ thông tin và các đối tượng cần bảo vệ trên địa bàn xã (Hệ thống mạng nội bộ, máy tính công vụ, hệ thống camera, phần mềm dùng chung,...);

+ Nhận diện, dự báo, đánh giá nguy cơ lây nhiễm mã độc, mất dữ liệu, lộ lọt thông tin, sự cố, phương thức tấn công mạng có thể xảy ra; đánh giá hậu quả, thiệt hại, mức độ tác động nếu xảy ra sự cố;

+ Kiểm tra việc cài đặt phần mềm phòng chống mã độc, cập nhật hệ điều hành, sao lưu dữ liệu.

+ Kiểm tra việc sử dụng tài khoản công vụ, mật khẩu, phân quyền truy cập.

- Đơn vị chủ trì: Văn phòng HĐND và UBND xã.

- Đơn vị phối hợp: Công an xã; Tổ ứng cứu sự cố an toàn thông tin mạng xã; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có) và các cơ quan, đơn vị có liên quan.

Thời gian thực hiện: Thường xuyên, tối thiểu 02 lần/năm.

2. Chủ động phòng ngừa và phát hiện sớm sự cố

- 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 của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố và tuân thủ theo các quy định, hướng dẫn.

- Nội dung thực hiện:

+ Triển khai các biện pháp phòng chống mã độc.

+ Theo dõi cảnh báo an toàn thông tin từ cơ quan chuyên trách cấp trên.

+ Thực hiện sao lưu dữ liệu định kỳ.

+ Tăng cường quản lý thiết bị USB, thư điện tử công vụ và tài khoản quản trị.

+ Tuyên truyền nâng cao nhận thức an toàn thông tin cho cán bộ, công chức.

Các nguy cơ thường gặp:

+ Tấn công mã độc, mã hóa dữ liệu;

+ Chiếm quyền điều khiển tài khoản;

+ Tấn công giả mạo, lừa đảo qua email;

+ Mất dữ liệu do lỗi thiết bị hoặc thao tác người dùng;

+ Sự cố mất điện, mất kết nối Internet;

+ Thiên tai, hỏa hoạn gây ảnh hưởng hệ thống CNTT.

- Đơn vị chủ trì: Văn phòng HĐND và UBND xã.

- Đơn vị phối hợp: Công an xã; các phòng, ban, đơn vị có liên quan; Tổ ứng cứu sự cố an toàn thông tin mạng xã; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có).

- Thời gian thực hiện: Thường xuyên hàng năm.

3. **Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố**

a) Báo cáo sự cố ATTT mạng:

- Đơn vị thực hiện: Đơn vị quản lý, vận hành hệ thống thông tin có trách nhiệm báo cáo ngay cho cơ quan chủ quản hệ thống thông tin, Công an xã và Tổ ứng cứu sự cố an toàn thông tin mạng xã khi xảy ra sự cố; việc báo cáo được duy trì trong suốt quá trình ứng cứu sự cố.

Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

b) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng:

- Đơn vị chủ trì: Công an xã; Văn phòng HĐND-UBND xã; Tổ ứng cứu sự cố an toàn thông tin mạng xã.

- Đơn vị phối hợp: Đội ứng cứu sự cố ATTT mạng tỉnh; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có) và các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo sự cố.

c) Quy trình ứng cứu sự cố ATTT mạng:

Thông thường và nghiêm trọng được thực hiện theo quy định tại Điều 13, Điều 14 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Điều 11 Thông tư số 20/2017/TT-BTTTT;

- Đơn vị chủ trì: Văn phòng HĐND UBND xã;

- Đơn vị phối hợp: Các phòng, ban, đơn vị, Tổ ứng cứu sự cố an toàn thông tin mạng xã.

- Thời gian thực hiện: Triển khai ngay sau khi tiếp nhận thông báo sự cố, đồng thời cập nhật, điều chỉnh quy trình hằng năm hoặc khi có thay đổi.

4. Triển khai nhiệm vụ phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố. Đồng thời cần đáp ứng đúng theo quy định tại Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ TTTT về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng, bao gồm:

a) Triển khai nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố:

- Nội dung thực hiện: Tăng cường giám sát, phát hiện sớm nguy cơ, sự cố; 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; đẩy mạnh tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Đơn vị chủ trì: Công an xã; Văn phòng HĐND và UBND xã; Tổ ứng cứu sự cố an toàn thông tin mạng xã.

Đơn vị phối hợp: Đội ứng cứu sự cố ATTT mạng tỉnh; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên, hàng năm.

b) Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố:

- Nội dung thực hiện: Mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố; chuẩn bị đầy đủ điều kiện về nhân lực, vật lực, tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của Đội ứng cứu sự cố và bộ phận ứng cứu sự cố; thuê dịch vụ kỹ thuật, 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 chủ trì: Công an xã; Văn phòng HĐND và UBND xã.

- Đơn vị phối hợp: Đội ứng cứu sự cố ATTT mạng tỉnh; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Hàng năm.

5. Quy trình ứng cứu sự cố an toàn thông tin mạng

Bước 1: Tiếp nhận và xác minh thông tin sự cố

- Tiếp nhận thông tin từ cán bộ, công chức hoặc hệ thống giám sát.
- Xác minh mức độ ảnh hưởng của sự cố.

Bước 2: Cô lập và xử lý ban đầu

- Ngắt kết nối thiết bị bị nhiễm mã độc khỏi mạng nội bộ.
- Sao lưu dữ liệu cần thiết.
- Thực hiện quét mã độc, thay đổi mật khẩu, khóa tài khoản nghi ngờ bị xâm nhập.

Bước 3: Phối hợp xử lý

- Báo cáo lãnh đạo UBND xã.
- Phối hợp Công an xã, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh và Đơn

vị cung cấp dịch vụ để xử lý.

Bước 4: Khôi phục hệ thống

- Khôi phục dữ liệu từ bản sao lưu.
- Kiểm tra an toàn trước khi đưa hệ thống hoạt động trở lại.

Bước 5: Báo cáo và rút kinh nghiệm

- Lập báo cáo sự cố.
- Đánh giá nguyên nhân, đề xuất biện pháp phòng ngừa tái diễn.

V. PHÂN CÔNG NHIỆM VỤ

1. Văn phòng HĐND - UBND xã

- Là đầu mối chịu trách nhiệm về ATTT mạng tại cơ quan, đơn vị theo thẩm quyền quản lý. Giao Chuyên viên Văn phòng HĐND và UBND phụ trách CNTT nhiệm vụ về ATTT mạng tại UBND xã.
- Xây dựng nội dung, lập dự toán kinh phí thực hiện các nhiệm vụ về ứng cứu, bảo đảm ATTT mạng tại UBND xã.
- Định kỳ 6 tháng và hàng năm hoặc đột xuất báo cáo cơ quan cấp trên tình hình ứng phó sự cố, bảo đảm ATTT mạng UBND xã.
- Tổ chức triển khai, xây dựng, quản lý, vận hành hạ tầng mạng, hạ tầng, nền tảng cơ sở dữ liệu dùng chung, phục vụ chuyển đổi số, ứng dụng CNTT. Phối hợp với Công an xã trong thực hiện công tác bảo đảm an toàn thông tin đối với hệ thống thông tin tập trung, dùng chung của xã.
- Tổ chức tuyên truyền, phổ biến kiến thức an toàn thông tin cho cán bộ, công chức.
- Theo dõi, tổng hợp tình hình sự cố và báo cáo UBND xã.

2. Công an xã

- Chủ trì phối hợp xử lý các sự cố an toàn thông tin mạng.
- Theo dõi tình hình an ninh mạng trên địa bàn.
- Phối hợp tuyên truyền, hướng dẫn kỹ năng bảo đảm an toàn thông tin.

3. Phòng Văn hóa - Xã hội, Trung tâm Dịch vụ tổng hợp

- Tổ chức tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn, các hoạt động liên quan đến bảo đảm ATTT mạng trên Trang thông tin điện tử, facebook và các phương tiện thông tin đại chúng.

4. Phòng Kinh tế

Căn cứ khả năng cân đối ngân sách xã, tham mưu cho cấp có thẩm quyền bố trí kinh phí thực hiện kế hoạch này theo quy định.

5. Các cơ quan, đơn vị

- Thực hiện nghiêm các quy định về bảo đảm an toàn thông tin.
- Kịp thời báo cáo khi phát hiện sự cố hoặc nguy cơ mất an toàn thông tin.
- Phối hợp trong quá trình xử lý, khắc phục sự cố.
- Cử cán bộ tham gia các chương trình huấn luyện, các khóa đào tạo, tập huấn về ứng cứu sự cố, bảo đảm ATTT mạng để nâng cao kỹ năng và công tác tham mưu, triển khai giám sát, bảo đảm ATTT mạng.

6.Doanh nghiệp viễn thông, CNTT

- Phối hợp hỗ trợ kỹ thuật khi xảy ra sự cố.
- Bảo đảm chất lượng đường truyền và an toàn hạ tầng dịch vụ.

VII. KINH PHÍ THỰC HIỆN

Nguồn kinh phí thực hiện Kế hoạch được bố trí từ ngân sách nhà nước theo phân cấp hiện hành và các nguồn kinh phí hợp pháp khác.

Trên đây là kế hoạch ứng phó sự cố, bảo đảm ATTT mạng tại UBND xã Cẩm Xuyên. UBND xã đề nghị các phòng, ban, đơn vị nghiêm túc triển khai thực hiện. Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc đề nghị phản ánh, kiến nghị về Văn phòng HĐND và UBND xã để tổng hợp, báo cáo UBND xã xem xét, quyết định./.

Nơi nhận:
- Công an tỉnh;
- Thường trực Đảng ủy, HĐND xã;
- Chủ tịch, các PCT UBND xã;
- Ủy ban MTTQ xã;
- Công an xã;
- Các phòng, ban chuyên môn;
- Trang TTĐT xã;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D XÃ CẨM XUYÊN HÀ TĨNH

Phan Trọng Bình