ỦY BAN NHÂN DÂN **XÃ KIM TÂN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 120 /KH-UBND	*Kim Tân, ngày 11 tháng 6 năm 2026*

KẾ HOẠCH
Ứng cứu sự cố, bảo đảm an toàn, an ninh mạng trên địa bàn xã Kim Tân

Thực hiện Kế hoạch số 150/KH-UBND ngày 19/5/2026 của UBND tỉnh Thanh Hóa về ứng cứu sự cố, bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh Thanh Hóa. UBND xã Kim Tân xây dựng Kế hoạch ứng cứu sự cố, bảo đảm an toàn, an ninh mạng trên địa bàn xã Kim Tân với các nội dung cụ thể như sau:

I. CĂN CỨ THỰC HIỆN

- Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;
- Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;
- Luật An ninh mạng ngày 12 tháng 6 năm 2018;
- Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;
- Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;
- Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 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;
- Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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;
- Quyết định số 964/QĐ-TTg ngày 10 tháng 8 năm 2022 của Thủ tướng Chính phủ phê duyệt chiến lược an toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức không gian mạng đến năm 2025, tầm nhìn 2030;
- Chỉ thị số 14/CT-TTg ngày 25 tháng 5 năm 2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng chống phần mềm độc hại;
- Chỉ thị số 14/CT-TTg ngày 07 tháng 6 năm 2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;
- Chỉ thị số 18/CT-TTg ngày 13 tháng 10 năm 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 09/CT-TTg ngày 23 tháng 02 năm 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;

- Chỉ thị số 60/CT-BTTTT ngày 16 tháng 9 năm 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.

II. MỤC ĐÍCH, YÊU CẦU VÀ QUY ĐỊNH CHUNG

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 chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin (ATTT) mạng; kịp thời khắc phục các tồn tại, lỗ hổng, điểm yếu nhằm phòng ngừa các sự cố tấn công mạng; đề ra các giải pháp ứng phó khi gặp sự cố mất ATTT mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về ATTT mạng đối với cán bộ, công chức, viên chức trong các cơ quan nhà nước của xã.

- Xây dựng, phát triển Tổ ứng cứu sự cố ATTT mạng xã có đầy đủ kiến thức, kỹ năng xử lý sự cố ATTT mạng bảo đảm linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.

- 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 ATTT mạng.

2. Yêu cầu

- Các hệ thống thông tin của các phòng, ban, ngành của xã phải được đánh giá hiện trạng và khả năng bảo đảm ATTT mạng, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra để đưa ra phương án ứng phó sự cố kịp thời, phù hợp.

- Hoạt động ứng cứu sự cố ATTT mạng phải chuyển từ bị động sang chủ động, bao gồm: Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý.

- 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 ATTT giữa các cơ quan nhà nước trên địa bàn xã; tận dụng sự phối hợp, hỗ trợ của cơ quan điều phối quốc gia về ứng cứu sự cố (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT).

3. Quy định chung

3.1. Phạm vi và đối tượng

Kế hoạch này để ứng phó sự cố, bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin của xã, áp dụng cho các phòng, ban, ngành, doanh nghiệp nhà nước; các cơ quan, đơn vị, doanh nghiệp có liên quan đến hoạt động ứng cứu sự cố ATTT mạng trên địa bàn xã.

3.2. Nguyên tắc, phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố ATTT mạng.

- Chủ động, kịp thời, nhanh chóng, chính xác; phối hợp chặt chẽ, đồng bộ và hiệu quả giữa các cơ quan, đơn vị.

- Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

- Thông tin trao đổi trong mạng lưới ứng phó sự cố ATTT mạng phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

- Bảo đảm bí mật thông tin khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của cơ quan điều phối quốc gia hoặc cơ quan, tổ chức, cá nhân gặp sự cố.

3.3. Các lực lượng tham gia ứng phó sự cố

- Các phòng, ban, doanh nghiệp có liên quan;

- Tổ ứng cứu sự cố ATTT mạng của xã (lực lượng chính ứng phó sự cố, trong đó Công an xã là cơ quan thường trực);

- Chủ quản hệ thống thông tin; đơn vị quản lý, vận hành hệ thống thông tin;

- Doanh nghiệp cung cấp dịch vụ viễn thông internet;

- Doanh nghiệp cung cấp dịch vụ ATTT mạng (trường hợp thuê dịch vụ);

- Trong trường hợp cần thiết, mời các cơ quan chức năng về ứng cứu sự cố cùng tham gia.

3.4. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các cơ quan đơn vị

- Công an xã Kim Tân: đơn vị chuyên trách ứng cứu sự cố ATTT mạng của xã; thực hiện chỉ đạo, tổ chức triển khai hoạt động ứng phó sự cố ATTT mạng và các nhiệm vụ khác khi xảy ra sự cố.

- Tổ ứng cứu sự cố ATTT mạng của xã: Lực lượng chính tham gia các hoạt động ứng cứu sự cố ATTT mạng; thực hiện nhiệm vụ theo Quy chế hoạt động của Tổ; tham gia hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng quốc gia khi có yêu cầu từ Công an xã hoặc các cơ quan có liên quan.

- Chịu trách nhiệm xây dựng, thực thi các quy định về an toàn bảo mật thông tin mạng, quản lý, khai thác, vận hành Trang thông tin điện tử xã; xử lý, ứng cứu các sự cố về an toàn thông tin, an ninh mạng xảy ra trên địa bàn xã khi có yêu cầu của đơn vị điều phối.

- Các cơ quan, đơn vị: Triển khai các nhiệm vụ theo chức năng, nhiệm vụ của đơn vị quản lý, vận hành hệ thống thông tin; Phối hợp với đơn vị chuyên trách ứng cứu sự cố ATTT mạng của xã (Công an xã) trong công tác ứng phó, xử lý các sự cố.

- Doanh nghiệp cung cấp, xây dựng các hệ thống thông tin: Phối hợp với Công an xã, chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin trong công tác ứng phó, xử lý các sự cố ATTT liên quan hệ thống thông tin do mình xây dựng hoặc cung cấp.

- Doanh nghiệp cung cấp dịch vụ viễn thông, internet: Phối hợp với Công an xã, chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin trong công tác ứng phó, xử lý các sự cố ATTT liên quan đến hạ tầng viễn thông, dịch vụ internet do mình cung cấp hoặc quản lý.

III. NỘI DUNG THỰC HIỆN

1. Đánh giá các nguy cơ, sự cố ATTT mạng

1.1. Đánh giá hiện trạng và nguy cơ

- Đánh giá hiện trạng và khả năng bảo đảm ATTT mạng của 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 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 (bao gồm cả đơn vị cung cấp dịch vụ nếu có).

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

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

- Thời gian thực hiện: Thường xuyên.

1.2. Chủ động rà quét, phát hiện và ngăn chặn mối nguy hại

- Chủ động thực hiện rà quét, phát hiện và ngăn chặn mối nguy hại và lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý; khắc phục các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng.

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

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

- Thời gian thực hiện: Hàng năm (tối thiểu 01 lần/06 tháng).

2. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi hệ thống thông tin, 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 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, bảo đảm các nội dung sau:

2.1. Quy trình triển khai và các bước ưu tiên ứng cứu ban đầu

Khi hệ thống thông tin gặp sự cố, có phân theo các loại sự cố thực hiện theo mục 3.3, Phần 3. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố của Kế hoạch này.

2.2. Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp

Các sự cố thường gặp bao gồm:

- Sự cố do bị tấn công mạng.

- 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 thiên tai, thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

2.3. Phương án đối phó, khắc phục sự cố đối với một hoặc nhiều tình huống

Tình huống sự cố do bị tấn công mạng bao gồm:

+ Tấn công từ chối dịch vụ;

+ Tấn công giả mạo;

+ Tấn công sử dụng mã độc;

+ Tấn công truy cập trái phép, chiếm quyền điều khiển;

+ Tấn công thay đổi giao diện;

+ Tấn công mã hóa phần mềm, dữ liệu, thiết bị;

+ Tấn công phá hoại thông tin, dữ liệu, phần mềm;

+ Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;

+ Tấn công tổng hợp sử dụng kết hợp nhiều hình thức;

Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật bao gồm:

+ Sự cố nguồn điện;

+ Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;

+ Sự cố đường kết nối internet;

+ 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 liên quan đến các thiên tai, thảm họa tự nhiên, như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất ATTT mạng khác.

2.4. Công tác tổ chức, điều hành, phối hợp giữa các lực lượng trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố

- Đơn vị chủ trì: Tiểu ban an toàn, an ninh mạng xã Kim Tân.

- Đơn vị phối hợp: Công an xã; Văn phòng HĐND và UBND xã; các ban, ngành, doanh nghiệp; Tổ ứng cứu sự cố ATTT mạng của xã; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên hàng năm.

2.5. Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ và dự kiến kinh phí để thực hiện đối phó, ứng cứu, xử lý đối với tình huống sự cố cụ thể

- Đơn vị chủ trì: Công an xã, các ban, ngành, doanh nghiệp trên địa bàn xã.

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

- Thời gian thực hiện: Thường xuyên hàng năm.

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

3.1. Báo cáo sự cố ATTT mạng

- Đơn vị thực hiện: Đơn vị quản lý, vận hành hệ thống thông tin báo cáo cơ quan chủ quản hệ thống thông tin, Công an xã, Tổ ứng cứu sự cố ATTT mạng của xã.

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

3.2. Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố ATTT mạng.

- Đơn vị chủ trì: Công an xã; đơn vị quản lý, vận hành hệ thống thông tin; Tổ ứng cứu sự cố ATTT mạng của xã.

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT; 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); các cơ quan, đơn vị chức năng liên quan.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố của tổ chức, cá nhân.

3.3. Quy trình ứng cứu sự cố ATTT mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTG của Thủ tướng Chính phủ và Điều 11 Thông tư 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Đơn vị chủ trì: Đơn vị vận hành hệ thống thông tin; Công an xã;

- Đơn vị phối hợp: Các ban, ngành, doanh nghiệp nhà nước;

- Thời gian thực hiện: Triển khai ngay sau khi tiếp nhận thông báo sự cố; cập nhật quy trình hàng năm hoặc khi có sự thay đổi.

4. Triển khai huấn luyện, diễn tập, 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, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố. Đồng thời cần đáp ứng theo quy định tại 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, bao gồm:

4.1. Triển khai các chương trình huấn luyện, diễn tập:

- Nội dung thực hiện: Tổ chức diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; huấn luyện, diễn tập 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, diễn tập vùng, miền, quốc gia, quốc tế.

- Đơn vị chủ trì: Công an xã; Tổ ứng cứu sự cố ATTT của xã;

- Đơn vị phối hợp: Đơn vị quản lý, vận hành hệ thống thông tin; Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT; các doanh nghiệp cung cấp dịch vụ viễn thông, internet; doanh nghiệp cung cấp dịch vụ ATTT (nếu có); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

4.2. Triển khai nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố

- Nội dung thực hiện: Thực hiện nghiêm công tác 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; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

- Đơn vị chủ trì: Công an xã; đơn vị quản lý, vận hành hệ thống thông tin; Tổ ứng cứu sự cố ATTT mạng của xã;

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT; các sở, ban, ngành, doanh nghiệp nhà nước; UBND tỉnh; các cơ quan, đơn vị chức năng có liên quan.

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

4.3. 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 các điều kiện bảo đảm, dự phòng 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 Tổ cứu sự cố, bộ phận ứng cứu sự cố; 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 chủ trì: Công an xã; các ban, ngành, doanh nghiệp nhà nước trên địa bàn xã.

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT; các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

IV. KINH PHÍ THỰC HIỆN

Nguồn kinh phí thực hiện Kế hoạch được bố trí từ nguồn ngân sách nhà nước theo phân cấp hiện hành; lồng ghép với kinh phí thực hiện các chương trình, kế hoạch, đề án khác có liên quan và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

V. TỔ CHỨC THỰC HIỆN

1. Các cơ quan, đơn vị, doanh nghiệp trên địa bàn xã

- Tổ chức triển khai thực hiện các nhiệm vụ về bảo đảm an toàn, an ninh mạng và ứng cứu sự cố an toàn thông tin mạng theo chức năng, nhiệm vụ được giao.

- Chủ động rà soát, phát hiện, xử lý hoặc phối hợp xử lý các nguy cơ, sự cố mất an toàn thông tin mạng thuộc phạm vi quản lý.

Cử cán bộ tham gia chương trình đào tạo, tập huấn, huấn luyện, diễn tập về bảo đảm an toàn thông tin mạng và ứng cứu sự cố theo kế hoạch của cấp có thẩm quyền.

- Phối hợp với Công an xã, Văn phòng HĐND và UBND xã trong công tác phòng ngừa, phát hiện, ứng cứu và khắc phục các sự cố an toàn thông tin mạng.

- Thực hiện chế độ thông tin, báo cáo định kỳ, đột xuất về tình hình bảo đảm an toàn thông tin mạng và ứng cứu sự cố theo quy định.

2. Công an xã

- Là cơ quan đầu mối, chuyên trách về ứng cứu sự cố an toàn thông tin mạng trên địa bàn xã, có trách nhiệm xây dựng và triển khai Kế hoạch này; tổ chức theo dõi, đôn đốc, phối hợp với các ban, ngành trong việc triển khai thực hiện Kế hoạch. Định kỳ 06 tháng, hàng năm hoặc đột xuất tổng hợp báo cáo kết quả thực hiện gửi UBND xã để theo dõi, chỉ đạo.

- Tham mưu UBND xã ban hành quyết định kiện toàn Tổ ứng cứu sự cố ATTT mạng cho phù hợp với tình hình bảo đảm ATTT trên địa bàn xã Kim Tân khi có sự thay đổi.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát, hướng dẫn công tác bảo đảm ATTT định kỳ hàng năm hoặc theo chỉ đạo của UBND xã đối với các cơ quan nhà nước, doanh nghiệp trên địa bàn xã. Tiến hành xử lý theo quy định của pháp luật các cá nhân, cơ quan vi phạm trong công tác bảo đảm ATTT mạng.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho hoạt động của Đơn vị chuyên trách ứng cứu sự cố và Tổ ứng cứu sự cố ATTT mạng của xã.

3. Văn phòng HĐND và UBND xã

- Là đầu mối tham mưu UBND xã trong quản lý, vận hành hệ thống thông tin, hạ tầng số, nền tảng số, cơ sở dữ liệu dùng chung và công tác bảo đảm an toàn thông tin mạng thuộc phạm vi quản lý của UBND xã.

- Giao công chức phụ trách công nghệ thông tin thực hiện nhiệm vụ về an toàn thông tin mạng theo quy định.

- Tổ chức triển khai, quản lý, vận hành hạ tầng mạng, nền tảng số, cơ sở dữ liệu dùng chung phục vụ công tác chỉ đạo, điều hành, chuyển đổi số của xã; phối hợp với Công an xã trong công tác bảo đảm an toàn thông tin mạng đối với các hệ thống thông tin dùng chung của xã.

- Chủ trì tham mưu thực hiện đánh giá, xác định cấp độ và lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định của pháp luật.

- Tổ chức tuyên truyền, phổ biến các quy định của pháp luật, hướng dẫn chuyên môn về an toàn thông tin mạng trên Trang thông tin điện tử và các kênh thông tin của xã.

- Cử cán bộ có trình độ, kinh nghiệm tham gia phối hợp xử lý, ứng cứu, khắc phục các sự cố an toàn thông tin mạng khi có yêu cầu của cơ quan có thẩm quyền.

- Thực hiện chế độ thông tin, báo cáo định kỳ, đột xuất về công tác bảo đảm an toàn thông tin mạng theo quy định.

- Kịp thời trao đổi, cung cấp thông tin liên quan đến các nguy cơ, sự cố an toàn thông tin mạng cho Công an xã để phối hợp theo dõi, xử lý theo quy định.

4. Phòng Văn hóa - Xã hội

Phối hợp với Công an xã phát huy thế mạnh về truyền thông phục vụ triển khai hiệu quả công tác thông tin tuyên truyền, phổ biến pháp luật về ATTT, an ninh mạng.

5. Phòng Kinh tế

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

Trên đây là Kế hoạch Ứng cứu sự cố, bảo đảm ATTT mạng trên địa bàn xã Kim Tân. Đề nghị các cơ quan, đơn vị nghiêm túc triển khai thực hiện. Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị phản ánh, kiến nghị về Công an xã hoặc Văn phòng HĐND và UBND xã để tổng hợp, báo cáo UBND xã, cấp có thẩm quyền xem xét, quyết định./.

Nơi nhận:
- Thường trực Đảng ủy, HĐND xã (để b/c);
- Chủ tịch, các PCT UBND xã (để b/c);
- Các phòng, ban chuyên môn;
- Công an xã;
- Ủy ban MTTQ và các đoàn thể xã;
- Các doanh nghiệp Viễn thông, CNTT trên địa bàn xã;
- Trang thông tin điện tử xã;
- Lưu: VT, VHXH.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

U.B.N.D XÃ KIM TÂN T.THANH HÓA

Bùi Thị Phúc

Phụ lục 01:

(Ban hành kèm theo Kế hoạch số: /KH-UBND ngày /6/2026 của UBND xã Kim Tân)

BÁO CÁO BAN ĐẦU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

I. Thông tin về tổ chức/cá nhân báo cáo sự cố

1. Tên tổ chức/cá nhân báo cáo sự cố: .....
2. Địa chỉ: .....
3. Điện thoại: .....; Email: .....

II. Người liên hệ

1. Họ và tên: .....; Chức vụ: .....
2. Điện thoại:.....; Email: .....

III. Thông tin chi tiết về hệ thống bị sự cố

Tên đơn vị đang quản lý, vận hành hệ thống thông tin (HTTT)	*Điền tên đơn vị quản lý, vận hành hoặc được thuê quản lý, vận hành hệ thống thông tin*
Cơ quan chủ quản HTTT	*Điền tên cơ quan chủ quản*
Tên HTTT xảy ra sự cố	*Điền tên hệ thống bị sự cố, tên miền, địa chỉ IP liên quan*
Phân loại cấp độ HTTT	☐ *Cấp độ 1* ☐ *Cấp độ 2* ☐ *Cấp độ 3* ☐ *Cấp độ 4* ☐ *Cấp độ 5*
Tổ chức cung cấp dịch vụ an toàn thông tin	*Điền tên nhà cung cấp dịch vụ an toàn thông tin*
Tên nhà cung cấp dịch vụ kết nối bên ngoài	*Điền tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)*
Dải IP Public kết nối hệ thống bên ngoài	*Điền thông tin dải IP công khai kết nối với hệ thống ra bên ngoài*

IV. Mô tả sơ bộ về sự cố

Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố: .....

.....

1. Ngày phát hiện sự cố (dd/mm/yyyy): .....

2. Thời gian phát hiện sự cố: *.....giờ.....phút.....giây.*

3. Hiện trạng sự cố: .....

.....

.....

☐ Đã được xử lý ☐Chưa được xử lý

4. Cách thức phát hiện:

☐ Qua hệ thống phát hiện xâm nhập

☐ Kiểm tra dữ liệu lưu lại (log file)

☐ Nhận được thông báo từ.....

☐ Nội dung khác: .....

.....

5. Đã gửi thông báo sự cố cho:

☐ Thành viên Đội ƯCSC ☐ Công an tỉnh

☐ Đơn vị xây dựng, phát triển hệ thống, dịch vụ, cổng/trang thông tin điện tử:.....

.....

.....

☐ Cơ quan chức năng có liên quan khác: .....

6. Thông tin bổ sung về hệ thống xảy ra sự cố:

a) Hệ điều hành:.....; Phiên bản:.....

b) Các dịch vụ có trên hệ thống: *(đánh dấu những dịch vụ có trên hệ thống)*

☐ Web Server ☐ Mail Server ☐ Database Server

☐ Dịch vụ khác: .....

c) Các giải pháp ATTT đã triển khai: *(Đánh dấu những giải pháp)*

☐ Antivirus ☐ Firewall ☐ Phòng chống xâm nhập

☐ Giải pháp khác:.....

d) Các địa chỉ IP của hệ thống: .....

e) Các tên miền của hệ thống:.....

f) Mục đích chính của hệ thống: .....

g) Thông tin gửi kèm: *(đánh dấu những dịch vụ có trên hệ thống)*

☐ Nhật ký hệ thống ☐ Mẫu virus, mã độc ☐ Danh sách IP

☐ Thông tin khác:.....

h) Thông tin cung cấp trong thông báo sự cố này phải giữ bí mật:

☐ Có ☐ Không

IV. Kiến nghị, đề xuất hỗ trợ

Mô tả tóm lược về kiến nghị, đề xuất được hỗ trợ (nếu có):

.....

.....

V. Thời gian thực hiện báo cáo sự cố: …./…./…./…./…. *(ngày/tháng/năm/giờ/phút)*

CÁ NHÂN/ĐẠI DIỆN THEO PHÁP LUẬT

(Ký tên, đóng dấu)

Phụ lục 02:

(Ban hành kèm theo Kế hoạch số: /KH-UBND ngày /6/2026 của UBND xã Kim Tân)

BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ ATTT MẠNG

I. Thông tin về tổ chức/cá nhân báo cáo sự cố

1. Tên tổ chức/cá nhân báo cáo sự cố: .....

2. Địa chỉ: .....

3. Điện thoại: .....; Email: .....

II. Ký hiệu báo cáo ban đầu sự cố: *Số ký hiệu/Ngày báo cáo (dd/mm/yyyy)*

III. Thông tin chi tiết về hệ thống bị sự cố

Tên đơn vị đang quản lý, vận hành HTTT	Điền tên đơn vị quản lý, vận hành hoặc được thuê quản lý, vận hành hệ thống thông tin
Cơ quan chủ quản HTTT	Điền tên cơ quan chủ quản
Tên HTTT xảy ra sự cố	Điền tên hệ thống bị sự cố, tên miền, địa chỉ IP liên quan
Phân loại cấp độ HTTT	☐ *Cấp độ 1* ☐ *Cấp độ 2* ☐ *Cấp độ 3* ☐ *Cấp độ 4* ☐ *Cấp độ 5*

IV. Tên/Mô tả sơ bộ về sự cố

Tóm tắt ngắn gọn về sự cố, diễn biến, mức độ, phạm vi ảnh hưởng:.....

.....

.....

.....

.....

1. Ngày phát hiện sự cố (dd/mm/yyyy):.....

2. Thời gian phát hiện sự cố: ..... giờ..... phút.....giây.

V. Các tài liệu đính kèm

Liệt kê, thống kê các tài liệu, báo cáo liên quan (tập tin, văn bản, hình ảnh, phương án xử lý, log file).....

.....

.....

CÁ NHÂN/ĐẠI DIỆN THEO PHÁP LUẬT

(Ký tên, đóng dấu)