

Số: 79 /KH-UBND

Nhơn Mỹ, ngày 10 tháng 4 năm 2026

KẾ HOẠCH
Ứng phó sự cố an toàn thông tin mạng
trên địa bàn xã Nhơn Mỹ

Thực hiện Kế hoạch số 149/KH-UBND ngày 03/4/2026 của Ủy ban nhân dân thành phố Cần Thơ về Ứng phó sự cố an toàn thông tin mạng trên địa bàn thành phố Cần Thơ.

Ủy ban nhân dân xã Nhơn Mỹ ban hành Kế hoạch Ứng phó sự cố an toàn thông tin mạng trên địa bàn xã, cụ thể 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 chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên 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 an toàn thông tin mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an ninh mạng, an toàn thông tin đối với cán bộ, công chức, viên chức trong các cơ quan nhà nước trực thuộc Ủy ban nhân dân xã.

- Xây dựng, phát triển Đội Ứng cứu sự cố an toàn thông tin mạng có đầy đủ kiến thức, kỹ năng xử lý sự cố an toàn thông tin mạng đảm bảo linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.

- Đảm bảo 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

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

- Hoạt động ứng cứu sự cố an toàn thông tin mạng phải chuyển từ bị động sang chủ động, bao gồm: chủ động thực hiện scan lỗ hổng mỗi 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 đảm bảo an toàn thông tin giữa các cơ quan nhà nước trên địa bàn thành phố; tăng cường sự phối hợp, hỗ trợ của cơ quan điều phối quốc gia về ứng cứu sự cố (VNCERT).

- Tham gia thường xuyên, đầy đủ các chương trình diễn tập tình huống hoặc thực chiến về ứng cứu sự cố an toàn thông tin mạng do các cơ quan chuyên trách tổ chức.

II. CÁC QUY ĐỊNH CHUNG

1. Phạm vi và đối tượng

Ứng phó sự cố an ninh mạng, an toàn thông tin đối với hệ thống thông tin các cơ quan, đơn vị, phòng ngành trực thuộc Ủy ban nhân dân xã và các tổ chức chính trị - xã hội trên địa bàn xã Nhơn Mỹ.

2. Nguyên tắc, phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an ninh mạng, an toàn thông tin mạng.

- Chủ động, kịp thời, nhanh chóng, chính xác; phối hợp chặt chẽ và 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 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. Các lực lượng tham gia ứng phó sự cố

- Các cơ quan, đơn vị, phòng ngành trực thuộc Ủy ban nhân dân xã và các doanh nghiệp có liên quan.

- Đội Ứng cứu sự cố an toàn thông tin mạng xã (cơ quan Thường trực là Văn phòng HĐND và UBND xã).

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

- Doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (trường hợp thuê dịch vụ).

- Trong trường hợp cần thiết, mời các cơ quan chuyên trách của các Sở, ngành thành phố có chức năng ứng cứu an ninh mạng, an toàn thông tin mạng cùng tham gia.

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

- Văn phòng HĐND và UBND xã: Đơn vị chuyên trách về an toàn thông tin mạng của xã; thực hiện chỉ đạo, tổ chức triển khai hoạt động ứng phó sự cố an toàn thông tin mạng và các nhiệm vụ khác khi xảy ra sự cố. Có trách nhiệm tổ chức quản lý, triển khai giám sát an toàn thông tin, cảnh báo về an toàn thông tin; là đầu mối điều phối kỹ thuật để xử lý thông tin vi phạm pháp luật trên không gian mạng theo quy định của pháp luật.

- Đội Ứng cứu sự cố an toàn thông tin mạng xã: Lực lượng chính tham gia các hoạt động ứng cứu sự cố an toàn thông tin mạng; thực hiện nhiệm vụ theo Quy chế hoạt động của Đội; tham gia hoạt động ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia khi có yêu cầu từ Công an thành phố hoặc các Sở, ngành có liên quan.

- Phòng Văn hóa - Xã hội xã: Chịu trách nhiệm xây dựng, thực thi các quy định về an toàn bảo mật thông tin mạng; tham gia Đội Ứng cứu sự cố an toàn thông tin mạng của 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, phòng ngành: Có trách nhiệm cử cán bộ, công chức, viên chức phụ trách an toàn thông tin tham gia Đội Ứng cứu sự cố an toàn thông tin mạng của xã khi xảy ra sự cố; phối hợp với đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng trong công tác ứng phó, xử lý các sự cố.

- Doanh nghiệp cung cấp, xây dựng các hệ thống thông tin: Phối hợp Văn phòng HĐND và UBND và 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 an toàn thông tin liên quan hệ thống thông tin do mình xây dựng hoặc cung cấp.

III. NỘI DUNG THỰC HIỆN

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

a) Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin 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: Đơn vị quản lý, vận hành hệ thống thông tin.

- Đơn vị phối hợp: Văn phòng HĐND và UBND; Công an; Phòng Văn hóa

- Xã hội xã; các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (trường

hợp thuê dịch vụ) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

b) Chủ động rà soát, phát hiện mối nguy và lỗ hổng bảo mật trong các hệ thống thông tin thuộc phạm vi quản lý; kịp thời khắc phục các điểm yếu theo cảnh báo của cơ quan chức năng, bảo đảm tuân thủ quy định tại Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ.

- Đơn vị chủ trì: Đơn vị quản lý, vận hành hệ thống thông tin.

- Đơn vị phối hợp: Văn phòng HĐND và UBND; Công an; Phòng Văn hóa

- Xã hội xã; các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (trường hợp thuê dịch vụ) 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, các phòng ngành, cơ quan, đơn vị 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 cần bảo đảm các nội dung:

a) 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 trường hợp cụ thể:

- 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 thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất an toàn thông tin mạng khác.

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

- Tình huống sự cố do bị tấn công mạng:

- + 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;
 - + Các hình thức tấn công mạng khác.
 - Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật:
 - + Sự cố nguồn điện;
 - + Sự cố đường kết nối Internet;
 - + Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;
 - + 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 do lỗi của người quản trị, vận hành hệ thống:
 - + Lỗi trong cập nhật, thay đổi, cấu hình phần cứng;
 - + Lỗi trong cập nhật, thay đổi, cấu hình phần mềm;
 - + Lỗi liên quan đến chính sách và thủ tục an toàn thông tin;
 - + Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc;
 - + Lỗi khác liên quan đến người quản trị, vận hành hệ thống.
 - Tình huống sự cố do lỗi từ người dùng cuối trong quá trình khai thác, sử dụng hệ thống:
 - + Chia sẻ thông tin, sử dụng chung tài khoản sai quy định;
 - + Lưu mật khẩu mặc định trên trình duyệt, làm lộ, mất thông tin đăng nhập;
 - + Không tuân thủ quy trình, quy chế, chính sách an toàn thông tin đã ban hành.
 - 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 an toàn thông tin mạng khác.
- c) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.
- Đơn vị chủ trì: Văn phòng HĐND và UBND xã.
 - Đơn vị phối hợp: Công an; các phòng ngành, cơ quan, đơn vị trực thuộc Ủy ban nhân dân xã; các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); các cơ quan, đơn vị khác có liên quan.
 - Thời gian thực hiện: Thường xuyên.
- d) 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 từng tình huống sự cố cụ thể.

- Đơn vị chủ trì: Các phòng ngành, cơ quan, đơn vị trực thuộc Ủy ban nhân dân xã.

- Đơn vị phối hợp: Công an xã; Đội Ứng cứu sự cố an toàn thông tin mạng xã; các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

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

a) Báo cáo sự cố an toàn thông tin mạng theo quy định tại Điều 11, Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ, Điều 9 Thông tư số 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Đơn vị thực hiện:

+ Đơn vị quản lý, vận hành hệ thống thông tin báo cáo cơ quan chủ quản hệ thống thông tin, Đội Ứng cứu sự cố an toàn thông tin mạng xã (qua Văn phòng HĐND và UBND); đồng gửi Ủy ban nhân dân thành phố (qua Công an thành phố - Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao).

+ Văn phòng HĐND và UBND xã báo cáo Chủ tịch Ủy ban nhân dân xã, Công an thành phố về 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 an toàn thông tin mạng theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Điều 10 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: Văn phòng HĐND và UBND xã; đơn vị quản lý, vận hành hệ thống thông tin (các cơ quan, đơn vị); Đội Ứng cứu sự cố an toàn thông tin mạng xã.

- Đơn vị phối hợp: Công an; Phòng Văn hóa - Xã hội xã; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; các doanh nghiệp cung cấp dịch vụ an toàn thông tin 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.

c) Quy trình ứng cứu sự cố an toàn thông tin 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: Đội Ứng cứu sự cố an toàn thông tin mạng xã.
- Đơn vị phối hợp: Các phòng ngành, cơ quan, đơn vị trực thuộc Ủy ban nhân dân xã; đơn vị quản lý, vận hành hệ thống thông tin.
- Thời gian thực hiện: Thường xuyên.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch được bố trí từ nguồn ngân sách hằng năm của xã bảo đảm cho hoạt động ứng phó sự cố an ninh mạng, an toàn thông tin và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

IV. TỔ CHỨC THỰC HIỆN

1. Các phòng ngành, cơ quan, đơn vị thuộc Ủy ban nhân dân xã

Căn cứ nội dung Kế hoạch này và tình hình thực tế tại cơ quan, đơn vị, xây dựng Kế hoạch Ứng phó sự cố an toàn thông tin mạng, nội dung theo hướng dẫn tại Phụ lục 3 của Thông tư 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) theo thẩm quyền quản lý và tổ chức triển khai các nhiệm vụ về ứng phó sự cố an toàn thông tin mạng theo đúng tiến độ, chất lượng, hiệu quả.

- Phân công lãnh đạo phụ trách; chỉ định bộ phận đầu mối; bố trí công chức, viên chức chuyên trách thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin tại cơ quan, đơn vị trong phạm vi quản lý. Khi có sự thay đổi cán bộ, công chức, viên chức chuyên trách về an toàn thông tin mạng tại cơ quan, đơn vị hoặc đang là thành viên tham gia Đội Ứng cứu sự cố an toàn thông tin mạng của xã thì đơn vị kịp thời thông báo về Ủy ban nhân dân xã (qua Văn phòng HĐND và UBND xã).

- Ưu tiên bố trí nguồn lực (*nhân lực, kinh phí*) và điều kiện để triển khai hoạt động ứng cứu sự cố an ninh mạng, an toàn thông tin trong hoạt động nội bộ của cơ quan, tổ chức và lĩnh vực quản lý. Xây dựng nội dung, lập dự toán kinh phí thực hiện các nhiệm vụ về ứng phó sự cố, bảo đảm an toàn thông tin của cơ quan, đơn vị mình hằng năm để tổ chức triển khai thực hiện, tránh chồng chéo, lãng phí.

- Thực hiện đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ).

- Định kỳ (06 tháng, 01 năm) hoặc đột xuất, các đơn vị báo cáo tình hình

ứng phó sự cố, bảo đảm an ninh mạng, an toàn thông tin trong phạm vi quản lý về Ủy ban nhân dân xã để tổng hợp báo cáo cấp trên theo quy định.

- Cử cán bộ tham gia đầy đủ các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn về ứng cứu sự cố, 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 mạng.

- 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 đảm bảo an ninh mạng của xã, của cơ quan, đơn vị trên các Trang thông tin điện tử, các phương tiện thông tin đại chúng: nội dung của Luật An an toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP; Thông tư số 12/2022/TT-BTTTT; các Công điện, Chỉ thị của Thủ tướng Chính phủ và các Chỉ thị, văn bản của Bộ Công an, Bộ Khoa học và Công nghệ.

2. Văn phòng HĐND và UBND xã

- Hằng năm tham mưu Ủy ban nhân dân xã ban hành Quyết định thành lập, kiện toàn Đội Ứng cứu sự cố an toàn thông tin mạng cho phù hợp với tình hình đảm bảo an toàn thông tin mạng trên địa bàn xã.

- Thực hiện trách nhiệm, quyền hạn của đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng theo Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) và Quyết định số 2214/QĐ-UBND ngày 04/11/2025 của Ủy ban nhân dân thành phố Cần Thơ.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát, hướng dẫn công tác bảo đảm an toàn thông tin định kỳ hằng năm hoặc theo chỉ đạo của Chủ tịch Ủy ban nhân dân xã đối với các cơ quan nhà nước trên địa bàn xã.

- Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo thẩm quyền quy định tại 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 (nay là Bộ Khoa học và Công nghệ).

- Định kỳ (06 tháng, 01 năm) hoặc đột xuất, tổng hợp báo cáo kết quả thực hiện ứng phó sự cố, bảo đảm an ninh mạng, an toàn thông tin trên địa bàn xã gửi Công an thành phố theo quy định.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho hoạt động của Đội Ứng cứu sự cố an toàn thông tin mạng của xã.

3. Phòng Văn hóa - Xã hội xã

- Nghiên cứu các giải pháp quản lý, vận hành hệ thống thông tin dùng chung

của thành phố; hướng dẫn các đơn vị truy cập, khai thác các hệ thống thông tin dùng chung của thành phố bảo đảm đúng quy định, đạt hiệu quả; chủ động phối hợp với Văn phòng HĐND và UBND, Công an xã duy trì giám sát, kịp thời phát hiện, xử lý khắc phục các điểm yếu, lỗ hổng bảo mật và triển khai các biện pháp phòng chống, ngăn chặn tấn công mạng, bảo đảm hệ thống thông tin vận hành thông suốt, ổn định.

- Trao đổi, chia sẻ kịp thời với các phòng ngành, cơ quan, đơn vị về thông tin liên quan đến sự cố mất an toàn thông tin mạng hệ thống thông tin tập trung, dùng chung của thành phố để chủ động phối hợp xử lý, ứng cứu khi cần thiết.

- Cử công chức có trình độ, kinh nghiệm tham gia 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.

- Phối hợp các phòng ngành, cơ quan, đơn vị triển khai thực hiện hiệu quả công tác tuyên truyền, phổ biến pháp luật và an toàn thông tin, an ninh mạng.

4. Phòng Kinh tế

Căn cứ khả năng cân đối của ngân sách xã, phối hợp với các cơ quan, đơn vị có liên quan tổng hợp, tham mưu Ủy ban nhân dân xã bố trí kinh phí để thực hiện Kế hoạch theo quy định của Luật Ngân sách nhà nước và các văn bản hướng dẫn liên quan.

Trong quá trình thực hiện nếu có khó khăn, vướng mắc, các phòng ngành, cơ quan, đơn vị báo cáo kịp thời về Ủy ban nhân dân xã (qua Văn phòng HĐND và UBND) để được chỉ đạo, giải quyết theo quy định. Giao Văn phòng HĐND và UBND xã chủ trì, giúp Chủ tịch Ủy ban nhân dân xã theo dõi, hướng dẫn, kiểm tra, đôn đốc việc thực hiện và tổng hợp báo cáo theo quy định./.

Nơi nhận:

- Công an thành phố;
- Sở KHCN thành phố;
- VP UBND thành phố;
- TT. Đảng ủy xã;
- TT. HĐND xã;
- TT. UBND xã;
- Công an xã;
- Các phòng ngành, đơn vị trực thuộc UBND xã;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH



Cao Minh Thơm