ỦY BAN NHÂN DÂN XÃ AN PHÚ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập -Tự do - Hạnh phúc
Số: 1104/QĐ-UBND	*An Phú, ngày 19 tháng 10 năm 2026*

QUYẾT ĐỊNH
Ban hành Quy trình ứng phó sự cố an ninh mạng hệ thống thông tin của Ủy ban nhân dân xã An Phú

ỦY BAN NHÂN DÂN XÃ AN PHÚ

Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15 ngày 16/6/2025;

Căn cứ Luật Giao dịch điện tử số 20/2023/QH15 ngày 22/6/2023;

Căn cứ Luật Dữ liệu số 60/2024/QH15 ngày 30/11/2024;

Căn cứ Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 ngày 26/6/2025;

Căn cứ Luật An ninh mạng số 116/2025/QH15 ngày 10/12/2025;

Căn cứ Luật Chuyển đổi số số 148/2025/QH15 ngày 11/12/2025;

Căn cứ Nghị định số 150/2025/NĐ-CP ngày 12/6/2025 của Chính phủ quy định tổ chức các cơ quan chuyên môn thuộc Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương và Ủy ban nhân dân xã, phường, đặc khu thuộc tỉnh, thành phố trực thuộc Trung ương đã được sửa đổi, bổ sung bởi Nghị định số 370/2025/NĐ-CP ngày 31/12/2025 của Chính phủ;

Căn cứ Nghị định số 356/2025/NĐ-CP ngày 31/12/2025 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật Bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 329/2026/NĐ-CP ngày 19/8/2026 của Chính phủ quy định về lực lượng bảo vệ an ninh mạng;

Căn cứ Nghị định số 330/2026/NĐ-CP ngày 19/8/2026 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng và bảo vệ dữ liệu cá nhân;

Căn cứ Nghị định số 331/2026/NĐ-CP ngày 19/8/2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin;

Căn cứ Nghị định số 332/2026/NĐ-CP ngày 19/8/2026 của Chính phủ quy định về hoạt động kinh doanh sản phẩm, dịch vụ an ninh mạng;

Căn cứ Nghị định số 333/2026/NĐ-CP ngày 19/8/2026 của Chính phủ quy định chi tiết một số điều và biện pháp thi hành Luật An ninh mạng;

Căn cứ 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;

Theo đề nghị của Chánh Văn Phòng HĐND và UBND.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy trình ứng phó sự cố an ninh mạng hệ thống thông tin của Ủy ban nhân dân xã An Phú.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký và thay thế các quyết định trước đây của Ủy ban nhân dân xã An Phú về ứng cứu, ứng phó sự cố an toàn thông tin, an ninh mạng.

Điều 3. Chánh Văn phòng HĐND và UBND xã; Trưởng phòng Văn hoá - Xã hội; Trưởng Công an xã An Phú; Thủ trưởng các cơ quan, đơn vị thuộc Ủy ban nhân dân xã An Phú; cán bộ, công chức, viên chức, người lao động và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- CATP (để báo cáo);
- Thường trực Đảng ủy;
- Thường trực HĐND xã;
- Lãnh đạo UBND xã;
- Công an xã;
- Lưu: VT, VP..

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D XÃ AN PHÚ T.P HẢI PHÒNG

Nguyễn Đình Dũng

ỦY BAN NHÂN DÂN XÃ AN PHÚ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY TRÌNH
Ứng phó sự cố an ninh mạng hệ thống thông tin của Ủy ban nhân dân xã An Phú

(Ban hành kèm theo Quyết định số 1104/QĐ-UBND ngày 19 tháng 10 năm 2026 của Ủy ban nhân dân xã An Phú)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Mục đích, yêu cầu

1. Mục đích

Quy trình này quy định nguyên tắc, tổ chức lực lượng, trách nhiệm, cơ chế chỉ đạo, điều phối, báo cáo và các bước xử lý khi xảy ra sự cố an ninh mạng đối với hệ thống thông tin (sau đây viết tắt là HTTT) thuộc phạm vi quản lý của Ủy ban nhân dân xã An Phú (sau đây gọi tắt là UBND xã An Phú), nhằm hạn chế tối đa thiệt hại, nhanh chóng khôi phục hoạt động quản lý, điều hành và cung cấp dịch vụ công cho tổ chức, công dân.

2. Yêu cầu

a) Việc ứng phó sự cố phải được thực hiện kịp thời, có tổ chức, đúng thẩm quyền, phù hợp với mức độ ảnh hưởng của sự cố và cấp độ HTTT.

b) Ưu tiên bảo vệ tính mạng, an toàn con người; tiếp theo là bảo vệ dữ liệu, tài sản thông tin và duy trì hoạt động của hệ thống, trước hết là các hoạt động phục vụ giải quyết thủ tục hành chính cho tổ chức, công dân.

c) Không tự ý xóa, sửa, cài đặt lại hoặc thay đổi dữ liệu, nhật ký và hiện trạng hệ thống liên quan đến sự cố khi chưa thực hiện các biện pháp cần thiết để bảo toàn thông tin phục vụ phân tích, điều tra.

d) Việc cô lập, ngắt kết nối hoặc tạm dừng một phần hoặc toàn bộ hệ thống phải được thực hiện trên cơ sở đánh giá mức độ ảnh hưởng và đúng thẩm quyền được giao.

đ) Sự cố vượt quá khả năng xử lý của UBND xã An Phú phải được báo cáo kịp thời Công an thành phố Hải Phòng (qua Phòng An ninh mạng) và có cơ chế phối hợp với các cơ quan, đơn vị chuyên môn, nhà cung cấp dịch vụ an ninh mạng theo quy định của pháp luật.

Điều 2. Phạm vi điều chỉnh và đối tượng áp dụng

1. Phạm vi điều chỉnh

Quy trình này quy định việc ứng phó sự cố an ninh mạng đối với các HTTT thuộc phạm vi quản lý của UBND xã An Phú theo Quy chế bảo vệ an ninh mạng trong hoạt động ứng dụng công nghệ thông tin và chuyển đổi số của UBND xã

An Phú. Đối với HTTT dùng chung do thành phố làm chủ quản hệ thống thông tin, UBND xã An Phú thực hiện xử lý ban đầu trong phạm vi quản lý và thông báo ngay cho chủ quản hệ thống thông tin để phối hợp xử lý.

2. Đối tượng áp dụng

a) Lãnh đạo UBND xã An Phú; Văn phòng HĐND và UBND, các phòng chuyên môn, Trung tâm Phục vụ hành chính công và các đơn vị thuộc UBND xã An Phú (sau đây gọi chung là các phòng, đơn vị); cán bộ, công chức, viên chức, người lao động thuộc UBND xã An Phú.

b) Công an xã An Phú.

c) Cơ quan, tổ chức, cá nhân có kết nối, sử dụng HTTT do UBND xã An Phú quản lý; tổ chức, doanh nghiệp cung cấp sản phẩm, dịch vụ công nghệ thông tin, dịch vụ an ninh mạng phục vụ hoạt động của UBND xã An Phú.

Điều 3. Nguyên tắc ứng phó sự cố an ninh mạng

1. Tuân thủ các quy định của pháp luật về điều phối, ứng phó sự cố an ninh mạng.

2. Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

3. Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các phòng, đơn vị, Công an xã An Phú và các cơ quan, tổ chức có liên quan.

4. Ứng phó sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ, trách nhiệm chính thuộc Đội ứng phó sự cố và Văn Phòng HĐND và UBND.

5. Thông tin trao đổi trong quá trình ứng phó phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo; không sử dụng kênh liên lạc nghi ngờ đã bị xâm phạm để trao đổi thông tin về sự cố.

6. Bảo đảm bí mật thông tin biết được khi tham gia, thực hiện các hoạt động ứng phó sự cố; chỉ người có thẩm quyền mới được cung cấp thông tin về sự cố cho cơ quan báo chí, tổ chức, cá nhân bên ngoài.

7. Dự phòng kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng phó sự cố; triển khai điều hành, phối hợp tổ chức ứng phó và thực hiện xử lý, ngăn chặn, khắc phục sự cố khi xảy ra.

8. Trường hợp sự cố có dấu hiệu liên quan đến tội phạm, xâm phạm an ninh quốc gia, bí mật nhà nước hoặc có nguy cơ gây ảnh hưởng nghiêm trọng đến hoạt động của UBND xã An Phú, phải ưu tiên bảo toàn hiện trường, thông tin, dữ liệu và chứng cứ phục vụ điều tra của cơ quan có thẩm quyền.

Điều 4. Đội ứng phó sự cố an ninh mạng

1. Tổ chức Đội ứng phó sự cố an ninh mạng

a) Chủ tịch UBND xã An Phú quyết định thành lập Đội ứng phó sự cố an ninh mạng của UBND xã An Phú (sau đây gọi tắt là Đội ứng phó sự cố).

b) Đội ứng phó sự cố phải có:

- Đội trưởng;

- Đội phó;

- Cán bộ làm đầu mối kỹ thuật và cán bộ dự phòng;

- Cán bộ làm đầu mối tiếp nhận, báo cáo sự cố và liên lạc;

- Cán bộ làm đầu mối thông tin, truyền thông;

- Các thành phần phối hợp khác có thể bao gồm: Đại diện các phòng, đơn vị có hệ thống, dữ liệu bị ảnh hưởng; đại diện đơn vị được thuê quản lý, vận hành hệ thống, doanh nghiệp viễn thông, nhà cung cấp sản phẩm, dịch vụ an ninh mạng khi cần thiết (nếu có).

c) Thành viên Đội ứng phó sự cố được xác định tại Quyết định thành lập Đội ứng phó sự cố; danh sách liên hệ và các đầu mối hỗ trợ bên ngoài được cập nhật ngay khi có thay đổi.

2. Chức năng, nhiệm vụ và cơ chế phối hợp

a) Đội trưởng chỉ đạo, điều phối hoạt động ứng phó sự cố; quyết định việc tạm dừng một phần hoặc toàn bộ HTTT do UBND xã An Phú quản lý khi cần thiết; quyết định báo cáo, đề nghị hỗ trợ từ cơ quan cấp trên.

b) Đội phó tham mưu, giúp việc cho Đội trưởng tổ chức thực hiện các hoạt động ứng phó; thay thế Đội trưởng điều hành khi Đội trưởng không thể thực hiện nhiệm vụ hoặc được uỷ quyền. Văn Phòng HĐND và UBND tham mưu về mặt kỹ thuật trong quá trình xử lý; tổng hợp thông tin, báo cáo Đội trưởng.

c) Công an xã An Phú hướng dẫn bảo toàn hiện trường, chứng cứ điện tử; tiếp nhận, xác minh, báo cáo Công an thành phố đối với sự cố có dấu hiệu vi phạm pháp luật, tội phạm.

d) Giao Văn Phòng HĐND và UBND phối hợp với nhà cung cấp dịch vụ: phát hiện, xác minh và xử lý kỹ thuật ban đầu; cô lập hoặc hạn chế phạm vi ảnh hưởng theo chỉ đạo; bảo toàn nhật ký và thông tin kỹ thuật; phân tích nguyên nhân; khắc phục và khôi phục hệ thống; cung cấp thông tin kỹ thuật phục vụ báo cáo.

đ) Người sử dụng hệ thống có trách nhiệm: thông báo ngay cho đầu mối được phân công; không tự ý xử lý theo cách có thể làm mất dữ liệu hoặc chứng cứ; không tự ý phát tán thông tin về sự cố; phối hợp với Đội ứng phó sự cố trong quá trình xử lý.

3. Đầu mối tiếp nhận, báo cáo sự cố

a) Đầu mối tiếp nhận sự cố của UBND xã An Phú là thành viên được phân công làm đầu mối tiếp nhận, báo cáo sự cố và liên lạc tại Quyết định thành lập Đội ứng phó sự cố. Số điện thoại tiếp nhận sự cố phải được duy trì liên lạc 24/7. Người tiếp nhận phản hồi xác nhận, báo ngay cho Đội trưởng; gửi thông báo, báo cáo sự cố đã được Đội trưởng phê duyệt đến Công an thành phố (qua Phòng An ninh mạng) và duy trì liên lạc trong suốt quá trình ứng phó. Đội ứng phó sự cố tổ chức việc tiếp nhận, ghi sổ theo dõi, tổng hợp và dự thảo thông báo, báo cáo sự cố.

b) Đầu mối tiếp nhận báo cáo sự cố của Công an thành phố Hải Phòng: Phòng An ninh mạng, đồng chí Nguyễn Thái Hoàng, số điện thoại 0978.763.468.

c) Khi có thay đổi thông tin đầu mối, Văn Phòng HĐND và UBND xã cập nhật ngay và thông báo đến các phòng, đơn vị, cán bộ, công chức, viên chức, người lao động và Công an thành phố; thông tin liên hệ được xác minh lại tối thiểu 01 lần/năm.

Chương II

PHÂN LOẠI VÀ ĐÁNH GIÁ NGUY CƠ SỰ CỐ AN NINH MẠNG

Điều 5. Phân loại mức độ sự cố an ninh mạng

1. Mức 0 (không): sự cố không gây ảnh hưởng có hại tức thời đến hoạt động và dữ liệu của hệ thống; tuy nhiên cần phân tích và báo cáo để tránh phát sinh sự cố khác trong tương lai.

2. Mức 1 (thấp): sự cố gây ảnh hưởng không đáng kể đến hoạt động hoặc dữ liệu của HTTT, gây tác động không đáng kể cho UBND xã An Phú hoặc cho xã hội (ví dụ: một máy trạm nhiễm mã độc đã được phần mềm phòng chống mã độc ngăn chặn).

3. Mức 2 (trung bình): sự cố gây ảnh hưởng đáng kể đến hoạt động hoặc dữ liệu của HTTT hoặc gây tác động đáng kể cho UBND xã An Phú hoặc cho xã hội (ví dụ: gián đoạn mạng nội bộ, gián đoạn tiếp nhận hồ sơ thủ tục hành chính trong thời gian ngắn; một số tài khoản bị chiếm quyền).

4. Mức 3 (nghiêm trọng): sự cố gây ảnh hưởng nghiêm trọng đến hoạt động của hệ thống, bao gồm ngừng hoạt động trong thời gian dài hoặc thiệt hại nghiêm trọng đến dữ liệu; gây tác động nghiêm trọng cho UBND xã An Phú hoặc ảnh hưởng tới trật tự xã hội, lợi ích công cộng, an ninh quốc gia (ví dụ: mã độc tống tiền mã hóa dữ liệu trên diện rộng; lộ, lọt dữ liệu cá nhân của công dân; Trang thông tin điện tử bị thay đổi giao diện, đăng tải nội dung xấu, độc).

5. Mức 4 (đặc biệt nghiêm trọng): sự cố làm tê liệt hoạt động của hệ thống hoặc thiệt hại đặc biệt nghiêm trọng tới dữ liệu; gây tác động đặc biệt nghiêm trọng cho UBND xã An Phú hoặc ảnh hưởng lớn tới trật tự xã hội, lợi ích công cộng, đe dọa nghiêm trọng tới an ninh quốc gia.

Sự cố từ Mức 0 đến Mức 2 được xác định là sự cố thông thường; sự cố Mức 3, Mức 4 hoặc sự cố vượt quá khả năng xử lý của UBND xã An Phú được xác định là sự cố nghiêm trọng.

Điều 6. Đánh giá các nguy cơ, sự cố an ninh mạng

1. Đội ứng phó sự cố chủ trì, Văn Phòng HĐND và UBND tham mưu, phối hợp với Công an xã An Phú định kỳ hằng năm thực hiện:

a) Đánh giá hiện trạng và khả năng bảo đảm an ninh mạng của các HTTT và các đối tượng cần bảo vệ;

b) Đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các HTTT;

c) Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố;

d) Đánh giá hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ ứng phó, khắc phục sự cố, bao gồm của cả nhà cung cấp dịch vụ đã ký hợp đồng (nếu có).

2. Các nguy cơ mất an ninh mạng chủ yếu đối với HTTT của UBND xã

a) Nguy cơ về khía cạnh vật lý: mất điện, nhiệt độ, độ ẩm không bảo đảm, sét đánh, hỏa hoạn, ngập lụt, thiên tai; thiết bị phần cứng bị hư hỏng, mất cắp, phá hoại.

b) Nguy cơ bị mất, hỏng, sửa đổi nội dung thông tin: người dùng vô tình để lộ mật khẩu hoặc không thao tác đúng quy trình, tạo cơ hội cho đối tượng xấu lấy cắp hoặc làm hỏng thông tin; đối tượng xấu sử dụng công cụ, kỹ thuật để thay đổi nội dung thông tin nhằm làm sai lệch thông tin của chủ sở hữu hợp pháp.

c) Nguy cơ bị tấn công bởi phần mềm độc hại: virus, sâu máy tính, phần mềm gián điệp, mã độc tống tiền… xâm nhập qua thư điện tử, thiết bị lưu trữ di động, phần mềm không rõ nguồn gốc, trang web độc hại.

d) Nguy cơ xâm nhập từ lỗ hổng bảo mật của hệ điều hành, phần mềm, thiết bị mạng, camera chưa được cập nhật bản vá hoặc đã hết hỗ trợ kỹ thuật.

đ) Nguy cơ xâm nhập do mật khẩu yếu, dùng chung, bị lộ: người dùng chia sẻ mật khẩu, ghi mật khẩu công khai, sử dụng mật khẩu mặc định trên thiết bị, cung cấp mã xác thực (OTP) cho đối tượng mạo danh.

e) Nguy cơ từ thư điện tử, tin nhắn, cuộc gọi lừa đảo: tấn công có chủ đích bằng thư điện tử, tin nhắn giả mạo cơ quan, lãnh đạo, đồng nghiệp hoặc đối tác, đính kèm tệp tin chứa mã độc hoặc liên kết tới trang web giả mạo nhằm đánh cắp tài khoản, cài đặt ứng dụng điều khiển từ xa.

g) Nguy cơ trong quá trình truyền tin: đối tượng xấu nghe lén, chặn bắt đường truyền, thay đổi hoặc phá hỏng nội dung thông tin khi truyền qua mạng không được mã hóa, mạng không dây công cộng.

h) Nguy cơ từ phần mềm điều khiển từ xa, truy cập trái phép của bên thứ ba, nhà cung cấp dịch vụ khi không được kiểm soát.

Chương III

QUY TRÌNH ỨNG PHÓ SỰ CỐ AN NINH MẠNG

Điều 7. Tiêu chí xây dựng phương án ứng phó sự cố

1. Đối với mỗi HTTT, Đội ứng phó sự cố chủ trì, Văn Phòng HĐND và UBND (thường trực Đội) tham mưu xây dựng tình huống, kịch bản sự cố cụ thể và phương án ứng phó tương ứng; kịch bản ứng phó đối với một số tình huống điển hình thực hiện theo tài liệu hướng dẫn do Văn Phòng HĐND và UBND ban hành.

2. Phương án ứng phó sự cố phải đặt ra các tiêu chí để nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố, bảo đảm các nội dung sau:

a) Quy trình triển khai và các bước ưu tiên ứng phó ban đầu khi HTTT gặp sự cố, có phân chia theo các loại sự cố.

b) Phương pháp, cách thức xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố: sự cố do bị tấn công mạng; sự cố do lỗi hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật, đường điện, đường truyền; sự cố do lỗi của người quản trị, vận hành hệ thống; sự cố liên quan đến thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn.

c) Phương án ứng phó, khắc phục đối với một hoặc nhiều tình huống sau:

- 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, Mạng truyền số liệu chuyên dùng; sự cố do lỗi phần mềm, phần cứng, ứng dụng; sự cố quá tải hệ thống; sự cố khác.

- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống: lỗi trong cập nhật, thay đổi, cấu hình phần cứng, phần mềm; lỗi liên quan đến chính sách và thủ tục an ninh mạng; lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc; lỗi do nhà cung cấp sản phẩm, dịch vụ; lỗi khác.

- Tình huống sự cố liên quan đến thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn.

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

Điều 8. Quy trình ứng phó sự cố an ninh mạng

Bước 1: Phát hiện và thông báo sự cố

a) Cán bộ, công chức, viên chức, người lao động tại các phòng, đơn vị khi phát hiện sự cố hoặc dấu hiệu bất thường (máy tính chạy chậm bất thường, xuất hiện thông báo đòi tiền chuộc, tệp tin bị đổi tên, mã hóa, cảnh báo của phần mềm phòng chống mã độc, tài khoản đăng nhập bất thường, Trang thông tin điện tử bị thay đổi nội dung…) thực hiện ngắt kết nối mạng của thiết bị (rút cáp mạng, tắt kết nối không dây; không tắt nguồn máy nếu không có hướng dẫn) để ngăn chặn lây lan, bảo đảm không làm mất các thông tin, nhật ký, dữ liệu cần thiết cho việc phân tích, điều tra.

b) Thông báo ngay cho đầu mối tiếp nhận sự cố tại khoản 3 Điều 4 Quy trình này bằng điện thoại hoặc trực tiếp; đồng thời báo cáo lãnh đạo phòng, đơn vị.

c) Không tự ý xóa dữ liệu, nhật ký, tệp tin, cài đặt lại hệ điều hành hoặc thực hiện các thao tác có khả năng làm mất dấu vết của sự cố; không tự ý liên hệ, trả tiền chuộc cho đối tượng tấn công.

d) Thông báo sự cố từ cơ quan, tổ chức bên ngoài (Công an thành phố, Sở Khoa học và Công nghệ, Cơ quan điều phối quốc gia, nhà cung cấp dịch vụ…) được Văn Phòng HĐND và UBND tiếp nhận và xử lý theo Quy trình này.

Bước 2: Tiếp nhận, xác minh và phân tích sơ bộ

a) Đầu mối tiếp nhận sự cố tiếp nhận thông tin, phản hồi xác nhận cho người thông báo và báo ngay cho Đội ứng phó sự cố; Đội ứng phó sự cố ghi nhận vào sổ theo dõi sự cố các thông tin: thời điểm phát hiện, người phát hiện, thiết bị, hệ thống bị ảnh hưởng, dấu hiệu sự cố.

b) Kiểm tra, xác minh để xác định thông tin tiếp nhận có phải là sự cố an ninh mạng hay không, gồm: tình trạng (sự cố sẽ xảy ra, đang xảy ra hay đã xảy ra); phạm vi (một máy tính, nhiều máy tính, toàn bộ mạng nội bộ, hệ thống dùng chung); địa điểm xảy ra sự cố.

- Trường hợp không phải sự cố: ghi nhận kết quả xác minh, hướng dẫn người dùng khắc phục (nếu cần) và đóng hồ sơ.

- Trường hợp xác định có sự cố: báo cáo ngay Đội trưởng, Đội phó và chuyển sang Bước 3.

Bước 3: Xử lý ứng cứu ban đầu

a) Đội ứng phó sự cố chủ trì, phối hợp với Văn Phòng HĐND và UBND, nhà cung cấp dịch vụ thực hiện các biện pháp cần thiết để hạn chế tác động và ngăn ngừa sự cố lan rộng. Tùy tính chất sự cố, có thể thực hiện:

- Cô lập thiết bị, máy chủ, tài khoản hoặc vùng mạng bị ảnh hưởng;

- Ngắt hoặc hạn chế các kết nối nghi ngờ; chặn địa chỉ IP, tên miền, dịch vụ liên quan đến sự cố;

- Khóa hoặc tạm khóa tài khoản có dấu hiệu bị chiếm quyền; thay đổi mật khẩu các tài khoản quản trị liên quan;

- Tạm dừng dịch vụ hoặc chức năng bị khai thác khi cần thiết;

- Ngăn chặn mã độc hoặc các hoạt động bất thường;

- Bảo vệ hệ thống sao lưu và các hệ thống chưa bị ảnh hưởng (ngắt kết nối thiết bị sao lưu khỏi mạng);

- Tăng cường giám sát các hệ thống, thiết bị và tài khoản có liên quan.

b) Thu thập, bảo toàn chứng cứ: chụp ảnh màn hình thông báo, ghi nhận thông tin hiện trạng; sao lưu nhật ký hệ thống, nhật ký tường lửa, nhật ký ứng dụng liên quan; lưu giữ mẫu tệp tin nghi ngờ trong môi trường cách ly. Biện pháp xử lý ban đầu phải bảo đảm không làm mất hoặc thay đổi trái phép các thông tin, nhật ký và chứng cứ cần thiết cho việc phân tích, điều tra.

c) Đối với sự cố trên HTTT dùng chung của thành phố, thông báo ngay cho đơn vị chủ quản, đơn vị vận hành hệ thống để phối hợp xử lý.

Bước 4: Phân loại, đánh giá mức độ sự cố

a) Đội ứng phó sự cố chủ trì, phối hợp với Văn Phòng HĐND và UBND đánh giá, phân loại sự cố theo Điều 5, Điều 6, Điều 7 Quy trình này và xác định phương án xử lý phù hợp.

b) Trên cơ sở đánh giá, xác định sự cố thuộc phạm vi ứng phó thông thường hay sự cố nghiêm trọng, vượt khả năng xử lý để thực hiện cơ chế báo cáo, đề nghị hỗ trợ và chuyển cấp xử lý.

c) Trường hợp sự cố dẫn đến hoặc có nguy cơ lộ, mất dữ liệu cá nhân của tổ chức, công dân, phải xác định loại dữ liệu, số lượng chủ thể dữ liệu bị ảnh hưởng để thực hiện thông báo theo quy định của pháp luật về bảo vệ dữ liệu cá nhân.

Bước 5: Báo cáo Lãnh đạo, xin ý kiến chỉ đạo và tổ chức ứng phó

Sau khi phân loại sự cố, Đội trưởng báo cáo Chủ tịch UBND xã An Phú đối với sự cố nghiêm trọng để xem xét, chỉ đạo xử lý.

a) Trường hợp sự cố thông thường:

- Đội ứng phó sự cố phối hợp với Văn Phòng HĐND và UBND tiếp tục triển khai các biện pháp xử lý nhằm kiểm soát sự cố, ngăn chặn sự cố tiếp tục phát sinh.

- Sau khi kiểm soát được sự cố, thực hiện loại bỏ nguyên nhân (gỡ bỏ mã độc, khắc phục điểm yếu, lỗ hổng đã bị khai thác, thu hồi quyền truy cập trái phép).

- Khôi phục hệ thống, dữ liệu theo thứ tự ưu tiên; chỉ đưa hệ thống trở lại hoạt động bình thường sau khi xác định nguyên nhân chính đã được kiểm soát và hệ thống đáp ứng yêu cầu an toàn.

- Đối với sự cố từ Mức 2 trở lên: báo cáo Công an thành phố (qua Phòng An ninh mạng) các nội dung: nguyên nhân sự cố, phạm vi ảnh hưởng, biện pháp khắc phục trong thời hạn 72 giờ kể từ thời điểm phát hiện sự cố.

b) Trường hợp sự cố nghiêm trọng:

- Đội trưởng Đội ứng phó sự cố chủ trì, phối hợp Văn Phòng HĐND và UBND và Công an xã tổng hợp và gửi báo cáo ban đầu đến Công an thành phố (qua Phòng An ninh mạng) trong thời hạn 24 giờ kể từ thời điểm phát hiện sự cố để kịp thời phối hợp đưa ra phương án ứng cứu; tổ chức ứng cứu, xử lý khẩn cấp; nghiêm túc chấp hành sự điều phối, hướng dẫn của Công an thành phố. Trường hợp sự cố có dấu hiệu xâm phạm an ninh quốc gia, trật tự, an toàn xã hội hoặc gây gián đoạn nghiêm trọng hoạt động của HTTT thì phải báo cáo ngay khi phát hiện.

- Duy trì báo cáo Lãnh đạo UBND xã An Phú, Công an thành phố trong suốt quá trình ứng phó theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg, gồm: báo cáo ban đầu; báo cáo diễn biến tình hình; báo cáo phương án ứng cứu cụ thể; báo cáo xin ý kiến chỉ đạo; báo cáo đề nghị hỗ trợ, phối hợp; báo cáo kết thúc ứng phó sự cố.

- Huy động các nguồn lực, điều phối các lực lượng tham gia ứng cứu khẩn cấp và thực hiện các bước tiếp theo quy định tại Điều 14 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ.

- Báo cáo Ủy ban nhân dân thành phố, chủ quản các HTTT dùng chung có liên quan để phối hợp xử lý.

c) Trường hợp sự cố lộ, mất dữ liệu cá nhân: ngoài báo cáo theo điểm a, điểm b Bước này, Đội ứng phó sự cố tham mưu UBND xã An Phú thông báo vi phạm quy định về bảo vệ dữ liệu cá nhân đến Công an thành phố Hải Phòng (qua Phòng An ninh mạng) chậm nhất 72 giờ kể từ thời điểm phát hiện theo quy định của Luật Bảo vệ dữ liệu cá nhân số 91/2025/QH15 và Nghị định số 356/2025/NĐ-CP; thông báo cho chủ thể dữ liệu bị ảnh hưởng trong trường hợp pháp luật quy định.

d) Trong quá trình xử lý sự cố, Văn phòng HĐND và UBND phối hợp Trung tâm Phục vụ hành chính công chủ động áp dụng phương án dự phòng (tiếp nhận hồ sơ trực tiếp, sử dụng thiết bị dự phòng đã được kiểm tra an toàn…) để bảo đảm không gián đoạn việc giải quyết thủ tục hành chính cho tổ chức, công dân; thông báo công khai về việc tạm dừng dịch vụ (nếu có) theo chỉ đạo của Lãnh đạo UBND xã An Phú.

Bước 6: Khôi phục, đánh giá kết quả, tổng kết và rút kinh nghiệm

a) Sau khi khôi phục hệ thống, Văn Phòng HĐND và UBND kiểm tra, đánh giá hoạt động của toàn bộ HTTT; trường hợp hệ thống chưa hoạt động ổn định, tiếp tục thu thập, xác minh lại nguyên nhân và tổ chức các bước tương ứng để xử lý dứt điểm.

b) Đội ứng phó sự cố chủ trì, phối hợp Văn Phòng HĐND và UBND, Công an xã, Công an thành phố và các đơn vị liên quan thu thập thông tin phục vụ phân tích sự cố; tổng hợp toàn bộ hồ sơ, báo cáo liên quan đến ứng phó sự cố để báo cáo Lãnh đạo UBND xã An Phú; gửi báo cáo kết thúc ứng phó sự cố đến cơ quan có thẩm quyền.

c) Đối với sự cố nghiêm trọng trừ Mức 3 trở lên, đơn vị tổ chức họp rút kinh nghiệm trong thời hạn 07 ngày làm việc kể từ khi kết thúc ứng phó; tổng kết nguyên nhân, bài học kinh nghiệm và đề xuất các biện pháp bổ sung về kỹ thuật, quản lý để hạn chế thiệt hại, tránh lặp lại sự cố tương tự trong tương lai; cập nhật Quy trình này, danh mục rủi ro và kịch bản ứng phó (nếu cần).

d) Hồ sơ sự cố (sổ theo dõi, biên bản, nhật ký, chứng cứ, báo cáo) được lưu trữ tại Văn Phòng HĐND và UBND phục vụ công tác kiểm tra, điều tra.

Chương IV

PHÒNG NGỪA, GIÁM SÁT, PHÁT HIỆN VÀ BẢO ĐẢM CÁC ĐIỀU KIỆN SẴN SÀNG ỨNG PHÓ, KHẮC PHỤC SỰ CỐ

Điều 9. Phòng ngừa sự cố và bảo đảm sẵn sàng ứng phó, khắc phục sự cố

1. Phòng ngừa và phát hiện sớm các nguy cơ, sự cố an ninh mạng

a) Giám sát, phát hiện và cảnh báo sớm: thực hiện giám sát thường xuyên đối với HTTT, hạ tầng mạng, thiết bị đầu cuối, thiết bị bảo mật, camera và các thành phần liên quan; thu thập, phân tích nhật ký để phát hiện dấu hiệu bất thường, truy cập trái phép, mã độc, khai thác lỗ hổng; tiếp nhận, xử lý kịp thời các cảnh báo của Công an thành phố, Sở Khoa học và Công nghệ, Cơ quan điều phối quốc gia và hệ thống giám sát tập trung của thành phố.

b) Kiểm tra, đánh giá và xử lý nguy cơ: thực hiện kiểm tra, đánh giá an ninh mạng theo kế hoạch; rà quét, phát hiện, xử lý lỗ hổng, điểm yếu; rà quét, cách ly, bóc gỡ mã độc; xử lý các thiết bị, tài khoản có dấu hiệu bị xâm nhập.

c) Quản lý rủi ro: nhận diện, phân tích, đánh giá và xử lý rủi ro an ninh mạng; theo dõi phương thức, thủ đoạn tấn công mới; chủ động triển khai biện pháp phòng ngừa trước khi phát sinh sự cố.

d) Hoàn thiện quy định và nâng cao nhận thức: xây dựng, cập nhật các quy chế, quy trình, hướng dẫn về bảo vệ an ninh mạng và ứng phó sự cố; tổ chức tuyên truyền, đào tạo cho cán bộ, công chức, viên chức, người lao động về phương thức tấn công mạng, mã độc, lừa đảo trực tuyến và trách nhiệm bảo vệ an ninh mạng.

2. Bảo đảm điều kiện sẵn sàng ứng phó và khắc phục sự cố

a) Công cụ, phương tiện: trang bị, duy trì và nâng cấp các thiết bị, công cụ, phần mềm phục vụ giám sát, phát hiện, ứng cứu và khắc phục sự cố; duy trì hiệu lực bản quyền phần mềm phòng chống mã độc, giải pháp bảo mật; chuẩn bị sẵn sàng máy tính dự phòng, thiết bị lưu trữ sạch, bộ cài đặt hệ điều hành, phần mềm hợp lệ; khi cần thiết, thuê dịch vụ giám sát, ứng cứu, khắc phục sự cố của tổ chức, doanh nghiệp đủ điều kiện theo quy định.

b) Nhân lực: phân công rõ trách nhiệm của các thành viên Đội ứng phó sự cố; duy trì danh sách liên hệ 24/7 và cơ chế huy động nhân lực khi xảy ra sự cố.

c) Dữ liệu và hạ tầng dự phòng: thực hiện sao lưu dữ liệu, cấu hình theo quy định; định kỳ kiểm tra khả năng khôi phục từ bản sao lưu; chuẩn bị phương án dự phòng về đường truyền, nguồn điện, thiết bị mạng.

d) Diễn tập: tham gia diễn tập bảo đảm an ninh mạng theo kế hoạch của thành phố, Bộ Công an; đánh giá, cập nhật phương án ứng phó sau diễn tập.

đ) Kinh phí: dự phòng kinh phí cho hoạt động ứng phó sự cố trong dự toán ngân sách hằng năm của UBND xã An Phú.

3. Tham gia Mạng lưới ứng phó sự cố an ninh mạng quốc gia

a) Thực hiện phối hợp, chia sẻ thông tin cảnh báo và hỗ trợ kỹ thuật về sự cố an ninh mạng theo quy định.

b) Tham gia các hoạt động của Mạng lưới ứng phó sự cố an ninh mạng quốc gia và các hoạt động phối hợp ứng phó sự cố do thành phố tổ chức.

c) Tiếp nhận, xử lý và phản hồi các cảnh báo, yêu cầu phối hợp ứng phó sự cố từ cơ quan có thẩm quyền.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 10. Tổ chức thực hiện

1. Quy trình này được áp dụng thống nhất trong hoạt động phòng ngừa, phát hiện, cảnh báo, ứng phó, khắc phục và phục hồi sau sự cố an ninh mạng đối với HTTT thuộc phạm vi quản lý của UBND xã An Phú.

2. Các phòng, đơn vị, cá nhân có liên quan có trách nhiệm thực hiện đúng chức năng, nhiệm vụ được phân công trong Quy trình này, bảo đảm việc xử lý sự cố được thực hiện kịp thời, có kiểm soát và hạn chế tối đa ảnh hưởng đến hoạt động của UBND xã An Phú.

3. Định kỳ hằng năm hoặc khi có thay đổi về hệ thống, tổ chức, quy định pháp luật, Văn Phòng HĐND và UBND rà soát, tham mưu UBND xã An Phú cập nhật Quy trình này.

Điều 11. Trách nhiệm của Văn Phòng HĐND và UBND

1. Là cơ quan thường trực của Đội ứng phó sự cố; tham mưu Đội ứng phó sự cố, phối hợp với Công an xã An Phú và các phòng, đơn vị xây dựng kế hoạch, phương án cụ thể thực hiện các nội dung tại Điều 5, Điều 6, Điều 7, Điều 8 Quy trình này.

2. Chủ trì, phối hợp với các phòng, đơn vị kiểm tra công tác bảo đảm an ninh mạng định kỳ hằng năm; xử lý, khắc phục các điểm yếu, lỗ hổng bảo mật, nguy cơ mất an ninh mạng theo hướng dẫn của Công an thành phố.

3. Tham mưu đưa nội dung dự phòng kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng phó sự cố vào các kế hoạch về bảo vệ an ninh mạng, chuyển đổi số hằng năm của UBND xã An Phú; tổ chức đào tạo cho thành viên Đội ứng phó sự cố và tham gia diễn tập theo kế hoạch của cơ quan có thẩm quyền.

Điều 12. Trách nhiệm của Công an xã An Phú

1. Phối hợp với Đội ứng phó sự cố, Văn Phòng HĐND và UBND trong tiếp nhận, xác minh, phân loại và xử lý sự cố; hướng dẫn bảo toàn hiện trường, chứng cứ điện tử.

2. Báo cáo Công an thành phố đối với các sự cố có dấu hiệu vi phạm pháp luật, tội phạm trên không gian mạng; phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng trong điều tra, xác minh, xử lý.

3. Phối hợp tuyên truyền, cảnh báo phương thức, thủ đoạn tấn công mạng, lừa đảo trực tuyến cho cán bộ, công chức, viên chức, người lao động.

Điều 13. Trách nhiệm của các phòng, đơn vị thuộc UBND xã An Phú

1. Phối hợp với Đội ứng phó sự cố, Văn Phòng HĐND và UBND, Công an xã và Công an thành phố trong quá trình ứng phó sự cố an ninh mạng; cử cán bộ, công chức tham gia khi được yêu cầu.

2. Tổ chức tuyên truyền, phổ biến các quy định nhằm nâng cao nhận thức, kiến thức, kỹ năng về an ninh mạng cho cán bộ, công chức, viên chức, người lao động thuộc phòng, đơn vị.

3. Tuân thủ Quy trình này; thông báo kịp thời các vấn đề bất thường liên quan tới an ninh mạng cho Đội ứng sự cố và Văn phòng HĐND và UBND; xây dựng phương án duy trì hoạt động nghiệp vụ khi HTTT bị gián đoạn.

Điều 14. Trách nhiệm của đơn vị cung cấp sản phẩm, dịch vụ công nghệ thông tin, an ninh mạng

1. Tuân thủ đầy đủ quy định của pháp luật về an ninh mạng, bảo vệ dữ liệu cá nhân và Nghị định số 332/2026/NĐ-CP.

2. Phối hợp xử lý sự cố theo phạm vi trách nhiệm và các điều khoản đã cam kết trong hợp đồng, thỏa thuận cung cấp dịch vụ; cử nhân sự kỹ thuật hỗ trợ khi được yêu cầu; cung cấp nhật ký, thông tin kỹ thuật cần thiết phục vụ phân tích, điều tra sự cố.

Trong quá trình thực hiện Quy trình này, nếu có vấn đề vướng mắc, phát sinh, các phòng, đơn vị phản ánh kịp thời về UBND xã An Phú (qua Văn Phòng HĐND và UBND) để tổng hợp, báo cáo xem xét điều chỉnh, bổ sung cho phù hợp./.