ỦY BAN NHÂN DÂN XÃ THẠNH LỘC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 2039/QĐ-UBND	*Thạnh Lộc, ngày 13 tháng 11 năm 2025*

QUYẾT ĐỊNH

Về việc ban hành Phương án ứng phó sự cố an ninh mạng cho các hệ thống thông tin của UBND xã Thạnh Lộc tỉnh An Giang

ỦY BAN NHÂN DÂN XÃ THẠNH LỘC

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2025;

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 Nghị định số 02/2025/NĐ-CP ngày 18/02/2025 của Chính phủ quy định về chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Công an;

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;

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

Theo đề nghị của Văn phòng HĐND – UBND xã tại Tờ trình số 21/TTr-VP ngày 10 tháng 11 năm 2025.

QUYẾT ĐỊNH:

Điều 1. Ban hành Phương án ứng phó sự cố an ninh mạng cho các hệ thống thông tin của UBND xã Thạnh Lộc tỉnh An Giang.

Điều 2. Quyết định có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng Hội đồng nhân dân và Ủy ban nhân dân xã, Thủ trưởng các cơ quan chuyên môn thuộc UBND xã, các cơ quan, đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Công an tỉnh (b/c);
- Sở Khoa học và Công nghệ (b/c);
- TT. Đảng ủy, HĐND, UBND, UBMTTQ xã;
- Văn phòng HĐND và UBND xã;
- Các Phòng, Trung tâm thuộc xã;
- Lưu: VT. lvrem.

CHỦ TỊCH

Tô Văn Tấn

PHƯƠNG ÁN
ỨNG PHÓ SỰ CỐ AN NINH MẠNG CHO CÁC HỆ THỐNG THÔNG TIN TRÊN ĐỊA BÀN XÃ THẠNH LỘC TỈNH AN GIANG

(Ban hành kèm theo Quyết định số 2034 /QĐ-UBND ngày 13 tháng 11 năm 2025 của Ủy ban nhân xã Thạnh Lộc)

CHƯƠNG I
QUY ĐỊNH CHUNG

Điều 1: Mục tiêu ban hành Phương án

Phương án ứng phó sự cố an ninh mạng được xây dựng nhằm:

- Chủ động phòng ngừa, phát hiện sớm, ứng phó kịp thời và khắc phục hậu quả của các sự cố an ninh mạng có thể xảy ra;

- Bảo đảm tính toàn vẹn, tính sẵn sàng và tính bảo mật của hệ thống thông tín, dữ liệu của tổ chức.

- Giảm thiểu tối đa thiệt hại và thời gian gián đoạn hoạt động khi xảy ra sự cố, thiết lập cơ chế phối hợp chặt chẽ với lực lượng chuyên trách về an ninh mạng, phục vụ hoạt động điều tra, xử lý và khôi phục, nâng cao năng lực phản ứng nhanh, điều tra số và khôi phục sau sự cố.

- Tuân thủ các quy định pháp lý hiện hành về an ninh mạng, an toàn thông tin.

Điều 2: Phạm vi áp dụng

- Áp dụng cho toàn bộ hệ thống thông tin, dữ liệu, tài nguyên số, ứng dụng, thiết bị phần cứng và phần mềm thuộc quản lý của tổ chức.

- Áp dụng cho tất cả cán bộ, công chức và các đơn vị liên quan có quyền truy cập hệ thống thông tin của tổ chức.

- Áp dụng đối với tất cả sự cố của hệ thống thông tin ở mọi cấp độ, từ mức độ sự cố đơn lẻ đến sự cố quy mô lớn, có yếu tố phá hoại, gián điệp hoặc ảnh hưởng tới an ninh quốc gia.

- Áp dụng cho cả hệ thống tại chỗ và hệ thống đám mây, mạng riêng ảo (VPN), mạng diện rộng (WAN), thiết bị đầu cuối, và hệ thống loT nếu có.

- Phạm vi áp dụng còn bao gồm các cơ quan, đơn vị trực thuộc UBND xã hoặc tổ chức liên kết đang sử dụng chung hạ tầng hệ thống thông tin với đơn vị chủ quan.

Điều 3: Giải thích từ ngữ

1. Sự cố an toàn thông tin mạng là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính khả dụng.

2. Sự cố an toàn thông tin mạng nghiêm trọng là sự cố đáp ứng đồng thời các tiêu chí sau:

- Hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 4, cấp độ 5 hoặc thuộc Danh mục hệ thống thông tin quan trọng quốc gia và bị một trong số các sự cố sau:

- Hệ thống bị gián đoạn dịch vụ; Dữ liệu tuyệt mật hoặc bí mật Nhà nước có khả năng bị tiết lộ: Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được.

- Hệ thống bị mất quyền điều khiển; Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin cấp độ 4 hoặc cấp độ 5 khác.

- Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý được sự cố.

3. Ứng cứu sự cố an toàn thông tin mạng là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm: theo dõi, thu thập, phân tích. phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

CHƯƠNG II

CÁC THÀNH PHẦN VÀ ĐẦU MỐI ỨNG CỨU SỰ CỐ

Các thành phần tổ chức triển khai việc ứng cứu sự cố an ninh mạng bao gồm: Đội ứng cứu sự cố an toàn thông tin mạng xã.

Điều 4: Thành lập Đội ,Tổ, Bộ phận ứng cứu sự cố nội bộ

- Chủ quản hệ thống thông tin thành lập Đội, Tổ, Bộ phận ứng cứu sự cố an ninh mạng nội bộ để thực hiện nhiệm vụ phát hiện, xử lý, phối hợp và khắc phục sự cố an toàn thông tin trong phạm vi sự cố. Đội ứng cứu sự cố có thể bao gồm đại diện từ các bộ phận sau: Văn phòng HĐND – UBND xã, Trung tâm Phục vụ hành chính công, Phòng Văn hóa – Xã hội, Công an xã.

- Đội ứng cứu sự cố hoạt động theo quy chế phối hợp nội bộ, chịu sự chỉ đạo chung của lãnh đạo đơn vị và phối hợp chặt chẽ với đầu mối điều phối ứng cứu.

- Đơn vị chỉ định rõ ràng đầu mối phục vụ điều phối ứng cứu sự cố, là cá nhân hoặc bộ phận chịu trách nhiệm: (1) Tiếp nhận thông tin về sự cố từ hệ thống giám sát, người dùng hoặc cảnh báo từ bên ngoài. (2) Kích hoạt quy trình ứng cứu, phân công nhiệm vụ và tổ chức triển khai biện pháp xử lý ban đầu; (3) Báo cáo cho Phòng PA05 và làm đầu mối liên hệ với các cơ quan chuyên trách về an ninh mạng: (4) Tổng hợp, báo cáo và cập nhật diễn biến sự cố theo đúng quy định.

- Trong trường hợp sự cố an ninh mạng có thể gây ảnh hưởng đến xã hội, yếu tố về truyền thông cần được tính toán kĩ lưỡng và có thể cần thông qua của nhiều cấp để giảm thiểu các rủi ro.

Điều 5: Trách nhiệm của các bộ phận liên quan, các đơn vị, bộ phận hoặc cá nhân có liên quan đến hệ thống thông tin tại đơn vị ứng cứu sự cố có trách nhiệm: (1) Phối hợp với đầu mối điều phối và Đội ứng cứu sự cố trong quá trình phát hiện, phân tích, cô lập và khắc phục sự cố; (2) Cung cấp đầy đủ, kịp thời thông tin, nhật

ký hệ thống, dữ liệu kỹ thuật, và các yếu tố liên quan phục vụ điều tra nguyên nhân sự cố; (3) Thực hiện nghiêm túc yêu cầu kỹ thuật, nghiệp vụ, bảo toàn hiện trạng hệ thống khi có yêu cầu từ lực lượng chuyên trách về an ninh mạng hoặc cơ quan điều phối ứng cứu sự cố.

Điều 6: Đội Ứng cứu sự cố an toàn thông tin mạng xã

- Đội Ứng cứu sự cố an toàn thông tin mạng xã có trách nhiệm tiếp nhận và xử lý sự cố an ninh mạng đối với các sự cố của các cơ quan, đơn vị khi được yêu cầu. Công an xã là đơn vị chủ trì tiếp nhận, điều phối hoạt động của Đội ứng cứu sự cố. Trong trường hợp không xử lý được, Đội ứng cứu sự cố an toàn thông tin mạng xã thực hiện báo cáo lên Đội ứng cứu an toàn thông tin tỉnh để nhận sự hỗ trợ.

Điều 7: Lực lượng chuyên trách đảm bảo an ninh mạng (Văn phòng HĐND – UBND xã) có trách nhiệm tiếp nhận thông tin báo cáo sự cố an ninh mạng, phối hợp với các Đội ứng cứu sự cố triển khai các công cụ và phương tiện cần thiết để thu thập chứng cứ số, dữ liệu để đánh giá thiệt hại theo các quy định của pháp luật (luật dữ liệu, luật bảo vệ dữ liệu cá nhân....) hướng dẫn các đơn vị xử lý sự cố đảm bảo theo yêu cầu pháp luật.

CHƯƠNG III

QUY TRÌNH ỨNG PHÓ SỰ CỐ

Điều 8: Phát hiện và báo cáo

- Khi phát hiện dấu hiệu bất thường trong hệ thống (thông qua giám sát, cảnh báo kỹ thuật hoặc phản ánh từ người dùng...), chủ quản hệ thống thông tin phải kịp thời kích hoạt quy trình ứng phó sự cố. Toàn bộ cán bộ, công chức có trách nhiệm thông báo sự cố tới đội phản ứng sự cố nội bộ (nếu đã được thành lập).

- Đơn vị vận hành hệ thống thông tin, đơn vị giám sát an ninh mạng có trách nhiệm báo cáo sự cố tới cơ quan chủ quản, đơn vị chuyên trách ứng cứu sự cố cùng cấp chậm nhất 12 giờ kể từ khi phát hiện sự cố (thời hạn này có thể thay đổi tùy thuộc vào điều khoản của hợp đồng trong trường hợp sử dụng các nhà cung cấp dịch vụ nhưng không được quá 12 giờ).

- Báo cáo sự cố phải được thực hiện ngay lập tức và được duy trì trong suốt quá trình ứng cứu sự cố 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, chỉ huy; báo cáo đề nghị hỗ trợ, phối hợp; báo cáo kết thúc ứng phó.

- Nội dung báo cáo cần bao gồm: Tên, địa chỉ đơn vị vận hành hệ thống thông tin, cơ quan chủ quản hệ thống thông tin, hệ thống thông tin bị sự cố, thời điểm phát hiện sự cố; đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố: mô tả về sự cố: Loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức, đơn vị cung cấp dịch vụ hạ tầng công nghệ thông tin, viễn thông; liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố, các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết qủa xử lý sự cố tính đến thời điểm báo cáo; kết quả ứng cứu sự cố ban đầu; kiến nghị đề xuất hưởng ứng cứu xử lý sự cố (nếu có).

Điều 9: Ứng phó ban đầu

- Ngay sau khi phát hiện sự cố, chủ quản hệ thống thông tin (Đội ứng cứu sự cố nội bộ) có trách nhiệm tiến hành ứng phó ban đầu nhằm hạn chế mức độ ảnh hưởng và có lập khu vực bị tác động, đồng thời giữ nguyên hiện trạng hệ thống và thực hiện theo hướng dẫn của cấp trên để phục vụ công tác điều tra (Công an xã có trách nhiệm yêu cầu thực hiện việc này đối với các sự cố nghi ngờ do tấn công mạng).

- Các hành động ưu tiên bao gồm: Cách ly hệ thống bị ảnh hưởng bằng cách ngắt kết nối mạng (nhưng không tắt nguồn hoặc khởi động lại thiết bị); ghi nhận các thông tin tại thời điểm xảy ra sự cố (tiến trình đang chạy, kết nối mạng. IP truy cập...); sao lưu nhật ký hệ thống (log), các file nghi ngờ, ảnh ổ đĩa, dữ liệu RAM theo đúng quy trình pháp y số.

- Đối với hệ thống không thể cách ly hoàn toàn, tìm các phương án chặn lọc kết nối của hệ thống với các IP nghi ngờ là độc hại.

- Trường hợp cần duy trì và khôi phục hoạt động của hệ thống bị ảnh hưởng, tiến hành việc chuyển sang hệ thống dự phòng hoặc khôi phục trên hạ tầng mới từ các bản sao lưu.

- Trong trường hợp nghi ngờ có yếu tố tấn công có chủ đích hoặc không đủ năng lực tự xử lý, chủ quản hệ thống thông tin phải đề nghị lực lượng chuyên trách về an ninh mạng trực tiếp phối hợp điều tra, hoặc chủ trì điều phối các doanh nghiệp an toàn thông tin chuyên nghiệp hỗ trợ xử lý. Khi đó, Công an xã triệu tập Đội ứng cứu sự cố an toàn thông tin mạng xã để hỗ trợ chủ quản xử lý sự cố.

- Trong quá trình xử lý sự cố, tăng cường việc giám sát an ninh mạng để phát hiện các hành vi tấn công mạng khác vào hệ thống, điều chỉnh phạm vi ảnh hưởng và kiểm tra hiệu quả của các biện pháp ngăn chặn đã thực hiện.

Điều 10: Phân tích và đánh giá mức độ nghiêm trọng ngày sau khi thực hiện các biện pháp ứng phó ban đầu, đội ngũ kỹ thuật và lực lượng chuyên trách sẽ tiến hành đánh giá sơ bộ và phân loại mức độ nghiêm trọng của sự cố:

- Mức 1. Phạm vi ảnh hưởng cục bộ, hệ thống vẫn có thể cung cấp dịch vụ, không có dữ liệu nhạy cảm bị truy cập – chủ quản hệ thống thông tin có thể xử lý nội bộ, thực hiện khắc phục theo quy trình sẵn có, thu thập dữ liệu theo yêu cầu và gửi báo cáo tổng kết kèm dữ liệu theo yêu cầu cho lực lượng chuyên trách sau khi hoàn tất.

- Mức 2. Ảnh hưởng trung bình, có gián đoạn cục bộ, nguy cơ rò rỉ dữ liệu người dùng hoặc chưa xác định rõ toàn bộ vùng bị tác động – chủ quản hệ thống thông tin phải phối hợp chặt chẽ với lực lượng chuyên trách để đánh giá hiện trạng và xác lập phạm vi ảnh hưởng. Trong trường hợp cần thiết, lực lượng chuyên trách có thể xem xét huy động sự hỗ trợ kỹ thuật từ doanh nghiệp an toàn thông tin nhằm hỗ trợ khoanh vùng, loại bỏ nguyên nhân và phục hồi hệ thống trong thời gian sớm nhất.

- Mức 3. Sự cố nghiêm trọng, có dấu hiệu phá hoại, lộ lọt tài liệu nội bộ, nhạy cảm, tấn công có chủ đích hoặc phạm vi ảnh hưởng vượt quá khả năng kiểm soát của chủ quản hệ thống thông tin – lực lượng chuyên trách về an ninh mạng giữ vai trò điều phối chính trong toàn bộ quá trình ứng phó, điều tra và khắc phục sự cố. Tùy theo tình hình cụ thể, lực lượng chuyên trách có thể triển khai các biện pháp kỹ thuật trực tiếp, đồng thời huy động lực lượng từ các doanh nghiệp cung cấp dịch vụ an toàn thông tin phù hợp để hỗ trợ khôi phục hệ thống trong thời gian ngắn nhất, đảm bảo duy trì hoạt động tối thiểu và giảm thiểu thiệt hại.

Điều 11: Thu thập dữ liệu, điều tra nguyên nhân sự cố

- Đơn vị chủ quản hệ thống thông tin được mời tham gia xử lý, khắc phục sự cố có trách nhiệm phối hợp chặt chẽ, cung cấp đầy đủ thông tin, tuân thủ các yêu cầu nghiệp vụ và kỹ thuật do lực lượng chuyên trách chỉ định, bao gồm cả việc bảo toàn hiện trạng phục vụ điều tra, hỗ trợ thu thập chứng cứ điện tử, cũng như triển khai các giải pháp phòng ngừa nguy cơ tái xâm nhập sau khi phục hồi.

- Xác định nguyên nhân sự cố là yêu cầu quan trọng của quá trình xử lý để khắc phục triệt để các yếu điểm gây ra sự việc. Các đơn vị theo phân công và trách nhiệm phân tích dữ liệu, thực hiện thêm các biện pháp kiểm thử (Pentest) trong trường hợp cần thiết để xác định rõ nguyên nhân.

Điều 12: Làm sạch và phục hồi

- Mục tiêu của giai đoạn này là loại bỏ hoàn toàn nguyên nhân sự cố, phục hồi hệ thống và đảm bảo an toàn khi vận hành trở lại.

- Các biện pháp xử lý có thể bao gồm: Gỡ bỏ mã độc, đóng các cổng dịch vụ bị khai thác, vá lỗ hổng, đổi mật khẩu, thu hồi tài khoản bị xâm nhập, cập nhật chính sách phân quyền, cấu hình lại hệ thống bảo mật. Hệ thống cần được phục hồi từ bản sao lưu sạch đã được kiểm tra tính toàn vẹn, tránh trường hợp khôi phục từ bản sao đã bị nhiễm mã độc. Trước khi đưa hệ thống trở lại hoạt động chính thức, chủ quản hệ thống thông tin phải thực hiện các bước kiểm tra độc lập, thử nghiệm kỹ thuật và tăng cường giám sát sau khôi phục.

- Lực lượng chuyên trách về an ninh mạng có trách nhiệm thực hiện công tác điều tra và xác minh trên cơ sở các dữ liệu, chứng cứ điện tử do chủ quản hệ thống thông tin cung cấp hoặc thu thập được trong quá trình xử lý sự cố; thực hiện xử lý theo quy định pháp luật trong trường hợp phát hiện dấu hiệu vi phạm; thực hiện đánh giá các yếu tố khác liên quan đến quy định của pháp luật (dữ liệu, bí mật nhà nước, dữ liệu cá nhân, kinh tế, xã hội...).

- Ngoài ra, lực lượng chuyên trách cần hướng dẫn chủ quản hệ thống thông tin bị ảnh hưởng triển khai biện pháp kỹ thuật tạm thời, hỗ trợ đảm bảo hoạt động tối thiểu, đồng thời đề xuất các kiến nghị nâng cao năng lực phòng thủ cho chủ quản hệ thống thông tin sau khi sự cố được kiểm soát.

Điều 13: Báo cáo hoàn tất và rút kinh nghiệm

- Sau khi sự cố đã được xử lý và hệ thống đi vào vận hành ổn định, chủ quản hệ thống thông tin có trách nhiệm hoàn thiện báo cáo kết quả xử lý sự cố gửi về lực

lượng chuyên trách an ninh mạng. Báo cáo cần nêu rõ nguyên nhân, quy trình xử lý, các biện pháp đã triển khai, đánh giá thiệt hại và đề xuất kiến nghị phòng ngừa. Đồng thời, chủ quản hệ thống thông tin phải tiến hành rút kinh nghiệm nội bộ, cập nhật quy trình ứng phó, điều chỉnh chính sách an toàn thông tin, bổ sung công cụ giám sát, khắc phục các lỗ hổng bảo mật và tổ chức tập huấn lại cho các bộ phận liên quan. Hồ sơ sự cố phải được lưu trữ đầy đủ, có chữ ký xác nhận, và bảo quản trong thời gian tối thiểu ba năm để phục vụ thanh tra, kiểm tra khi cần thiết.

- Dựa vào phương án, các đơn vị xây dựng các kịch bản ứng phó sự cố an ninh mạng cho các hệ thống, ưu tiên các hệ thống thông tin quan trọng và các loại sự cố an ninh mạng ảnh hưởng đến các yếu tố quan trọng của hệ thống (ví dụ ransomware; lộ lọt dữ liệu đối với các hệ thống văn bản quan trọng, lưu trữ dữ liệu cá nhân; deface đối với các cổng thông tin,...).

CHƯƠNG IV

TỔ CHỨC THỰC HIỆN

Điều 14: Trách nhiệm của UBND xã

- Chủ trì, phối hợp với các đơn vị liên quan thực hiện các nội dung theo quy định của phương án này.

- Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn xã.

- Chủ trì, điều phối các thành viên của Đội ứng cứu sự cố an toàn thông tin mạng phối hợp với các Đội, Tổ, Bộ phận ứng cứu sự cố nội bộ thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố và bảo đảm an toàn thông tin mạng, ứng dụng công nghệ thông tin.

- Thường xuyên kiểm tra việc thực hiện phương án ứng cứu sự cố cho các hệ thống thông tin. Thường xuyên tổ chức các cuộc tập huấn, 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 cho chủ quản các hệ thống thông tin, đơn vị vận hành, quản lý, sử dụng các hệ thống thông tin trên địa bàn xã.

- Phối hợp với Công an tỉnh trong trường hợp không xử lý được các vấn đề phức tạp, nghiêm trọng để nhận sự hỗ trợ.

Điều 15. Trách nhiệm thi hành

- Đơn vị chủ quản hệ thống thông tin trên địa bàn xã có trách nhiệm phổ biến, quán triệt đến toàn bộ cán bộ, công chức trong đơn vị thực hiện các quy định của phương án ứng cứu sự cố an ninh mạng cho hệ thống thông tin.

Trong quá trình thực hiện, nếu có những vấn đề khó khăn, vướng mắc, các đơn vị liên hệ UBND xã (qua Công an xã tổng hợp, trình các cấp có thẩm quyền xem xét, sửa đổi, bổ sung phương án cho phù hợp)./.