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

PHƯƠNG ÁN
ỨNG PHÓ SỰ CỐ AN NINH MẠNG CHO CÁC HỆ THỐNG THÔNG TIN ỦY BAN NHÂN DÂN XÃ AN BIÊN

(Ban hành kèm theo Quyết định số 2596/QĐ-UBND ngày 17 tháng 11 năm 2026 của Ủy ban nhân dân xã An Biên)

I. MỤC TIÊU BAN HÀNH PHƯƠNG ÁN

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

1. 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.

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

3. Giảm thiểu tối đa thiệt hại và thời gian gián đoạn hoạt động khi xảy ra sự cố.

4. 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, nâng cao năng lực phản ứng nhanh, điều tra số và khôi phục sau sự cố.

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

II. PHẠM VI, ĐỐI TƯỢNG VÀ HỆ THỐNG ÁP DỤNG

1. Phương án áp dụng đối với cán bộ, công chức, viên chức, người lao động, người được giao quản trị hoặc vận hành hệ thống, nhà thầu và tổ chức, cá nhân được cấp quyền truy cập hệ thống thông tin thuộc phạm vi quản lý, sử dụng của UBND xã và các cơ quan, đơn vị trên địa bàn khi xử lý công việc.

2. Hệ thống, thiết bị trong phạm vi áp dụng gồm máy tính và thiết bị đầu cuối; mạng nội bộ, đường truyền Internet và mạng truyền số liệu chuyên dùng; thư điện tử công vụ, hệ thống quản lý văn bản, chữ ký số; trang thông tin điện tử xã do Văn phòng HĐND và UBND xã quản trị; dữ liệu, tài khoản, phần mềm

nghiệp vụ, thiết bị lưu trữ, thiết bị mạng và dịch vụ công nghệ thông tin được giao quản lý hoặc sử dụng.

3. Đối với nền tảng, cơ sở dữ liệu hoặc dịch vụ do tỉnh, bộ, ngành hay nhà cung cấp quản lý tập trung, xã chỉ xử lý thiết bị, tài khoản và kết nối thuộc phạm vi của mình; đồng thời thông báo ngay cho đơn vị chủ quản, vận hành để phối hợp. Không tự ý thay đổi cấu hình, truy cập máy chủ hoặc khôi phục dữ liệu của hệ thống dùng chung khi chưa được đơn vị có thẩm quyền hướng dẫn.

4. Không áp dụng đối với hệ thống thông tin chuyên dùng của Công an xã, Ban Chỉ huy Quân sự xã và hệ thống cơ yếu, hệ thống xử lý bí mật nhà nước; các hệ thống này thực hiện phương án, quy trình chuyên ngành. Khi có sự cố ảnh hưởng đến thiết bị, tài khoản hoặc hệ thống dùng chung với UBND xã, các bên thông báo và phối hợp theo thẩm quyền.

III. CÁC THÀNH PHẦN VÀ ĐẦU MỐI ỨNG CỨU SỰ CỐ

Tổ chức ứng cứu sự cố an ninh mạng thuộc thẩm quyền quản lý của Ủy ban nhân dân xã An Biên bao gồm:

- Cơ quan đầu mối phối hợp về ứng cứu sự cố an toàn thông tin mạng của xã là Công an xã An Biên. Công an xã là lực lượng nòng cốt của UBND xã trong công tác phối hợp bảo đảm an ninh mạng (cán bộ được phân công phụ trách công nghệ/chuyển đổi số của Công an xã).

- Hoạt động ứng cứu, xử lý và khắc phục sự cố mất an toàn thông tin mạng đối với các hệ thống thông tin thuộc phạm vi quản lý của Ủy ban nhân dân xã An Biên theo quy định của pháp luật.

1. 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 có 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, Công an xã, Trung Tâm Phục vụ Hành Chính công, Phòng Văn hóa – Xã hội, Phòng kinh tế.

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 bộ phận an ninh mạng – Công an xã 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.

2. 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 sự cố tỉnh để nhận sự hỗ trợ.

3. 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 điều phối 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.

4. Lực lượng chuyên trách đảm bảo an ninh mạng

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.

IV. QUY TRÌNH ỨNG PHÓ SỰ CỐ

1. 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...) cán bộ, công chức có trách nhiệm thông báo sự cố tới cơ quan đầu mối phối hợp về ứng cứu sự cố an toàn thông tin mạng của xã là Công an xã An Biên. Công an xã là lực lượng nòng cốt của UBND xã trong công tác phối hợp bảo đảm an ninh mạng và đội ứng cứu sự cố an toàn thông tin mạng của Ủy ban nhân dân xã. Chậm nhất 12 giờ kể từ khi phát hiện 4 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).

- 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, kết quả ứng cứu sự cố ban đầu; kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có).

2. Ứng phó ban đầu

- Ngay sau khi phát hiện sự cố, chủ quản hệ thống thông tin (Đội ứng cứu sự cố) có trách nhiệm tiến hành ứng phó ban đầu nhằm hạn chế mức độ ảnh hưởng và cô 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 nghỉ ngờ, ảnh ổ đĩa, dữ liệu RAM theo đúng quy trình pháp y số.

- 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. 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.

3. Phân tích và đánh giá mức độ nghiêm trọng

Ngay 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, 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.

- *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.

4. 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.

5. 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.

6. 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, chu 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 khuyến 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.

V. TỔ CHỨC THỰC HIỆN

1. 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.

- 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.

2. Công an xã

- 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.

- 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.

3. Các cơ quan, đơn vị thuộc xã

- Thủ trưởng đơn vị trực tiếp chỉ đạo xử lý trong phạm vi quản lý; cử cán bộ tham gia lực lượng ứng cứu nội bộ; cung cấp thông tin hệ thống, nhật ký, danh sách tài khoản và tình trạng dữ liệu; triển khai biện pháp kỹ thuật theo hướng dẫn của đầu mối xã, đơn vị vận hành và cơ quan chuyên trách. Mỗi đơn vị phải cập nhật đầu mối liên hệ khi xảy ra sự cố an toàn thông tin mạng.

4. Cán bộ phụ trách công nghệ thông tin và người sử dụng

Cán bộ phụ trách công nghệ thông tin hướng dẫn cô lập thiết bị, thu thập thông tin kỹ thuật ban đầu, không tự ý xóa dữ liệu, cài lại hệ điều hành hoặc thay đổi cấu hình làm mất dấu vết. Người sử dụng báo ngay khi thấy dấu hiệu bất thường, làm theo hướng dẫn và không tự phát tán thông tin sự cố.

5. Nhà cung cấp dịch vụ

Khi được liên hệ, nhà cung cấp phối hợp xác minh, cô lập nguồn tấn công, khôi phục dịch vụ, cung cấp nhật ký và báo cáo kỹ thuật; chỉ thực hiện thao tác trên hệ thống theo yêu cầu của chủ quản hoặc đơn vị vận hành có thẩm quyền và hướng dẫn của cơ quan chức năng.

6. 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 Văn phòng HĐND và UBND xã tổng hợp), trình các cấp có thẩm quyền xem xét, sửa đổi, bổ sung phương án cho phù hợp)./.