

Số: /PA-UBND

Cư Yang, ngày tháng 8 năm 2026

PHƯƠNG ÁN

Ứng cứu sự cố bảo đảm an toàn thông tin mạng trên địa bàn xã Cư Yang

Thực hiện Công văn số 1323/UBND-VP ngày 12/8/2026 của UBND xã Cư Yang và Công văn số 423-CV/ĐU ngày 07/8/2026 của Đảng ủy xã Cư Yang về triển khai Kết luận của đồng chí Bí thư Tỉnh ủy – Trưởng Tiểu ban An ninh mạng tỉnh Đắk Lắk. UBND xã Cư Yang xây dựng phương án ứng cứu sự cố bảo đảm an ninh mạng trên địa bàn xã Cư Yang cụ thể như sau:

I. CÁC QUY ĐỊNH CHUNG

1. Phạm vi và đối tượng

Phương án này để ứng phó sự cố, bảo đảm an toàn thông tin mạng (sau đây gọi tắt là ATTTM) đối với các hệ thống thông tin (gọi tắt là HTTT) của Ủy ban nhân dân các xã Cư Yang (gọi tắt là UBND xã).

2. Nguyên tắc, phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng phó sự cố ATTTM.
- Chủ động, kịp thời, nhanh chóng, chính xác; phối hợp chặt chẽ, đồng bộ và hiệu quả giữa các cơ quan, đơn vị.
- Ứng phó sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản HTTT.
- 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 phó 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

- Chủ quản hệ thống thông tin; Đơn vị quản lý, vận hành HTTT.
- Các phòng chuyên môn thuộc UBND xã, Công an xã, Quân sự xã, các cơ quan, đơn vị, doanh nghiệp có liên quan (VNPT, điện lực, ...).
- Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đắk Lắk (sau đây gọi tắt là Đội UCSC).

II. NỘI DUNG THỰC HIỆN

1. Các nội dung, nhiệm vụ thực hiện thường xuyên, chủ động phòng ngừa sự cố xảy ra

- Thường xuyên tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về ATTTM.
- Tham gia các chương trình đào tạo, bồi dưỡng kỹ năng đánh giá, ứng phó khẩn cấp sự cố.
- Bố trí công chức đủ năng lực chuyên môn, có phẩm chất tốt để vận hành HTTT.
- Đầu tư, gia hạn bản quyền phần mềm, thiết bị, công cụ, phương tiện phục vụ ứng phó, khắc phục sự cố.

2. Một số tình huống sự cố cụ thể

2.1. 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.

2.2. Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật

- Nguồn điện;
- Đường kết nối Internet;
- Do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin;
- Liên quan đến quá tải hệ thống;
- Do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

2.3. 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 ATTTM;
- 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.

2.4. 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 ATTTM khác.

3. Triển khai các nội dung, nhiệm vụ khi có sự cố xảy ra

Triển khai hoạt động theo Quy trình ứng cứu sự cố ATTTM thông thường và nghiêm trọng, thực hiện một số nội dung cụ thể sau:

3.1. Báo cáo sự cố ATTTM

- Đơn vị vận hành hệ thống thông tin có trách nhiệm báo cáo sự cố tới cơ quan chủ quản hệ thống (UBND xã), Công an tỉnh, Đội UCSC.

- Báo cáo sự cố phải được thực hiện ngay lập tức (khi phát hiện) và được duy trì trong suốt quá trình ứng phó sự cố gồm: báo cáo ban đầu; báo cáo diễn biến tình hình; báo cáo phương án ứng phó 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.

- Hình thức báo cáo thông qua kênh trao đổi Signet của thành viên Đội UCSC tại UBND xã hoặc bằng công văn, thư điện tử theo mẫu phụ lục 2 đính kèm.

Nguyên tắc báo cáo, trao đổi thông tin trong ứng phó sự cố: Đơn vị vận hành hệ thống thông tin báo cáo Chủ quản hệ thống thông tin, Công an tỉnh; thành viên Đội UCSC tại UBND xã trao đổi với Chủ quản hệ thống thông tin, báo cáo Công an tỉnh.

3.2. Xử lý ban đầu sự cố ATTTM

- Đơn vị vận hành HTTT khi phát hiện hoặc nhận được thông báo sự cố đối với HTTT do mình quản lý, phải thực hiện:

- Ghi nhận, tiếp nhận thông báo, báo cáo sự cố và tập hợp các thông tin liên quan theo đúng quy trình.

- Phản hồi cho tổ chức, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được đề xác nhận về việc đã nhận được thông báo, báo cáo sự cố.

- Chủ trì, phối hợp cùng đơn vị cung cấp dịch vụ ATTTM (nếu có), Đội UCSC và các đơn vị chức năng liên quan tiến hành phân tích, xác minh, đánh giá tình hình sơ bộ, phân loại sự cố, triển khai ngay các hoạt động ứng phó sự cố và báo cáo theo quy định.

- Báo cáo về sự cố, diễn biến tình hình ứng phó sự cố, đề xuất hỗ trợ ứng phó sự cố hoặc nâng cấp nghiêm trọng của sự cố (khi cần) cho chủ quản HTTT và Công an tỉnh.

3.3. Triển khai các biện pháp ứng phó, khắc phục, xử lý sự cố

a) Đơn vị vận hành, chủ quản HTTT phối hợp thực hiện các biện pháp ứng phó ban đầu:

Xử lý nhanh ban đầu: (1) Thực hiện cách ly hệ thống (máy chủ/máy trạm lưu trữ dữ liệu quan trọng) khỏi hệ thống mạng; nhanh chóng thực hiện lưu trữ dữ

liệu quan trọng vào thiết bị điện tử chuyên dụng (đã được kiểm tra chứng nhận bảo đảm ATTTM); (2) Tạm dừng các ứng dụng dịch vụ quan trọng trong hệ thống mạng (nếu cần thiết), bảo vệ an toàn máy chủ, thiết bị lưu trữ dữ liệu chuyên dụng.

Đánh giá ban đầu về sự cố: (1) Do lỗi nguồn điện; (2) Do lỗi đường truyền Internet; (3) Do lỗi phần mềm, phần cứng, ứng dụng của HTTT; (4) Do lỗi của hệ thống (thiết bị, phần mềm, hạ tầng kỹ thuật); (5) Từ ảnh hưởng của thảm họa tự nhiên: cháy nổ, mưa bão, lũ lụt...; (6) Bị tấn công mạng.

b) Tiến hành các biện pháp khôi phục tạm thời

Căn cứ vào mục tiêu được ưu tiên trong khắc phục sự cố, đơn vị Chủ quản HTTT phối hợp với các nhà cung cấp dịch vụ, Đội UCSC và các cơ quan chức năng khác tiến hành khôi phục một số hoạt động, dữ liệu hoặc kết nối cần thiết nhất để giảm thiểu thiệt hại đối với HTTT, tránh làm ảnh hưởng đến uy tín của cơ quan chủ quản, quản lý hệ thống hoặc gây ảnh hưởng xấu tới xã hội.

Chủ quản HTTT phải phối hợp chặt chẽ, cung cấp đầy đủ thông tin để Công an tỉnh thực hiện giám sát, theo dõi quá trình phục hồi và diễn biến tiếp theo, ảnh hưởng trong thời gian chưa khắc phục triệt để sự cố.

Xử lý hậu quả ban đầu: Chủ quản HTTT cần nhanh chóng tiến hành các biện pháp khắc phục khẩn cấp các hậu quả, thiệt hại do tấn công mạng gây ra làm ảnh hưởng đến người dân, xã hội, cơ quan, tổ chức khác theo yêu cầu của Công an tỉnh.

c) Báo cáo, phối hợp với Đội UCSC xác định nguyên nhân sự cố:

Tình huống sự cố do bị tấn công mạng: (1) Tấn công từ chối dịch vụ; (2) Tấn công giả mạo; (3) Tấn công sử dụng mã độc; (4) Tấn công truy cập trái phép, chiếm quyền điều khiển; (5) Tấn công thay đổi giao diện; (6) Tấn công mã hóa phần mềm, dữ liệu, thiết bị; (7) Tấn công phá hoại HTTT, dữ liệu, phần mềm; (8) Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; (9) Tấn công tổng hợp sử dụng kết hợp nhiều hình thức; (10) Các hình thức tấn công mạng mới, khác.

Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống: (1) Lỗi trong cập nhật, thay đổi, cấu hình phần cứng; (2) Lỗi trong cập nhật, thay đổi, cấu hình phần mềm; (3) Lỗi liên quan đến chính sách và thủ tục an toàn thông tin; (4) Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc; (5) Lý do khác liên quan đến trách nhiệm được quy định đối với người quản trị, vận hành hệ thống.

Tình huống sự cố do lỗi xuất phát từ người dùng cuối (quá trình truy cập, khai thác vào hệ thống): (1) Chia sẻ thông tin, sử dụng chung tài khoản sai quy định định; (2) Làm lộ, mất thông tin tài khoản; (3) Thực hiện sai các hướng dẫn

đã ban hành về quy trình, quy chế, chính sách và thủ tục an toàn thông tin người dùng.

d) Phối hợp với Đội UCSC triển khai, thực hiện các biện pháp ứng phó, xử lý khắc phục sự cố:

Xác định phạm vi đối tượng, mục tiêu cần ưu tiên ứng phó; thực hiện ứng phó theo thứ tự mức độ quan trọng (thành phần chức năng, ứng dụng dịch vụ, dữ liệu quan trọng cần bảo vệ, khôi phục).

Tìm hiểu về các sự cố tương tự, có liên quan đã xảy ra, phân tích, tìm giải pháp ứng phó, xử lý khắc phục hiệu quả nhất.

Phân loại, thực hiện ứng phó mục tiêu: khôi phục hoạt động, bảo đảm bí mật dữ liệu (bảo đảm tính toàn vẹn dữ liệu, hạn chế mức thấp nhất mức độ thất thoát dữ liệu).

Chia sẻ thông tin, tài liệu liên quan đến tình huống ứng phó cho các thành viên tham gia theo chức năng, nhiệm vụ được giao.

Nhận định diễn biến tình hình và phương thức thủ đoạn tấn công (nếu có), dự đoán các diễn biến tiếp theo có thể xảy ra; xây dựng phương án, xác định biện pháp ngăn chặn tấn công mạng, hướng đến việc xác minh thông tin, truy vết đối tượng tấn công.

Cảnh báo sự cố trên mạng lưới ứng phó của tỉnh, các đơn vị có liên quan, kịp thời phòng tránh xảy ra các sự cố tương tự.

e) Một số biện pháp xử lý, khắc phục sự cố khẩn cấp:

Khắc phục sự cố, gỡ bỏ mã độc: (1) Sao lưu hệ thống trước và sau khi xử lý sự cố; (2) Tiêu diệt các mã độc, phần mềm độc hại; (3) Khôi phục hệ thống, dữ liệu và kết nối; (4) Cấu hình hệ thống an toàn; (5) Kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố; (6) Khắc phục các điểm yếu an toàn thông tin; (7) Bổ sung các thiết bị, phần cứng, phần mềm bảo vệ an toàn thông tin cho hệ thống; (8) Triển khai theo dõi, giám sát, ngăn chặn khả năng lặp lại sự cố hoặc xảy ra các sự cố tương tự.

Ngăn chặn, xử lý hậu quả: Chủ quản HTTT có trách nhiệm xử lý các hậu quả do sự cố HTTT của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác. Các đơn vị thuộc thành phần tham gia tác nghiệp ứng phó khẩn cấp, dựa trên các kết quả phân tích, điều tra, sử dụng các nguồn lực, phương tiện và nghiệp vụ của mình để tiến hành ngăn chặn các hành vi gây ra sự cố và hỗ trợ xử lý, khắc phục hậu quả.

III. PHÂN CÔNG NHIỆM VỤ

1. Văn phòng HĐND & UBND

- Tham mưu Chủ tịch UBND xã phân công lãnh đạo phụ trách hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về ATTTM tại UBND xã theo thẩm quyền quản lý.

- Bố trí công chức chuyên trách về ATTTM tại UBND xã; kịp thời thông báo về Công an tỉnh khi có sự thay đổi công chức chuyên trách về ATTTM tại UBND xã hoặc đang là thành viên tham gia Đội UCSC của tỉnh.

- Thực hiện đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn HTTT theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn HTTT theo cấp độ và theo hướng dẫn tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng 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 HTTT theo cấp độ.

- Định kỳ 06 tháng và hằng năm, hoặc đột xuất báo cáo tình hình ứng phó sự cố, bảo đảm ATTTM tại UBND xã về Công an tỉnh để tổng hợp báo cáo các cơ quan cấp trên theo quy định.

- Cử cán bộ, công chức tham gia các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn về ứng phó sự cố, bảo đảm ATTTM để nâng cao kỹ năng và công tác tham mưu, triển khai giám sát, bảo đảm ATTTM.

2. Phòng Kinh tế

Phối hợp với các phòng chuyên môn xây dựng nội dung, dự toán kinh phí thực hiện các nhiệm vụ về ứng phó sự cố, bảo đảm ATTTM, lồng ghép trong Kế hoạch chuyển đổi số của UBND xã.

3. Phòng Văn hóa - Xã hội

Triển khai 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 ATTTM của tỉnh, của cơ quan đơn vị trên Trang thông tin điện tử, các phương tiện thông tin đại chúng: nội dung của Luật An toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông; các Công điện, Chỉ thị của Thủ tướng Chính phủ và các Chỉ thị.

4. Trách nhiệm các phòng chuyên môn, các trung tâm các đơn vị sự nghiệp thuộc UBND xã

Quan tâm, chú trọng đến công tác bảo đảm ATTTM tại đơn vị mình quản lý.

Phối hợp với Văn phòng HĐND&UBND xã và các đơn vị liên quan thực hiện công tác ứng phó khi xảy ra sự cố ATTTM.

IV. TỔ CHỨC THỰC HIỆN

1. Căn cứ nội dung phương án này các phòng chuyên trách, các cơ quan đơn vị thuộc UBND xã thực hiện nghiêm các nội dung được phân công tổ chức triển khai các nhiệm vụ về ứng phó sự cố an ninh mạng theo đúng tiến độ, chất lượng, hiệu quả.

2. Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các phòng chuyên môn phản ánh kịp thời về Văn phòng HĐND và UBND để tổng hợp tham mưu cho UBND xã xem xét giải quyết theo đúng quy định của pháp luật./.

Nơi nhận:

- UBND tỉnh Đắk Lắk;
- Công an tỉnh Đắk Lắk;
- Đảng ủy xã;
- Thường trực HĐND xã;
- Chủ tịch, các Phó Chủ tịch UBND xã;
- Công an xã;
- Ban Chỉ huy Quân sự xã;
- Văn phòng HĐND&UBND xã;
- Phòng Văn hóa - Xã hội;
- Phòng Kinh tế;
- Trung tâm Phục vụ hành chính công xã;
- Các trường học trên địa bàn xã;
- Trung tâm cung ứng dịch vụ sự nghiệp công xã Cư Yang.
- Lưu: VT

CHỦ TỊCH

Trần Văn Đông

