ỦY BAN NHÂN DÂN **XÃ NGUYỄN NGHIÊM**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**

PHƯƠNG ÁN
Ứng phó sự cố, bảo đảm an toàn thông tin đối với Hệ thống mạng LAN phục vụ công tác chỉ đạo điều hành, hoạt động nội bộ đơn vị Uỷ ban nhân dân Xã Nguyễn Nghiêm
(Kèm theo Quyết định số: 432 /QĐ-UBND ngày 14 /8/2025 của Chủ tịch Ủy ban nhân dân Xã Nguyễn Nghiêm)

I. MỤC ĐÍCH, YÊU CẦU

1. Phương án này hướng dẫn việc ứng cứu sự cố hệ thống thông tin, trách nhiệm của các phòng chuyên môn, trung tâm và cá nhân có liên quan đến đảm bảo an toàn, an ninh thông tin đối với Hệ thống mạng LAN của đơn vị Ủy ban nhân dân Xã Nguyễn Nghiêm *(gọi tắt là Trung tâm).*

2. Chủ động thực hiện kiểm tra, rà quét lỗ hổng hệ thống thông tin trong phạm vi quản lý nhằm phòng ngừa, chủ động, ứng phó kịp thời, khắc phục khẩn trương và hiệu quả các sự cố xảy ra.

3. Nâng cao năng lực xử lý tình huống sự cố tại chỗ của các phòng, ban và Trung tâm.

4. Tăng cường thông tin, tuyên truyền, cảnh báo, hướng dẫn các biện pháp phòng, tránh ứng phó sự cố hệ thống thông tin nhằm phát huy ý thức tự giác, chủ động ứng phó của công chức tại các phòng, ban và Trung tâm.

II. NHIỆM VỤ TRỌNG TÂM

1. Phòng Văn hóa - Xã hội chịu trách nhiệm trước Chủ tịch Ủy ban nhân dân xã trong việc ứng cứu sự cố an toàn thông tin của Ủy ban nhân xã, như sau:

a) Tham mưu tổ chức triển khai, hướng dẫn, kiểm tra, đôn đốc việc thực hiện phương án này.

b) Chủ trì, phối hợp với các phòng, ban và Trung tâm thường xuyên kiểm tra, đề xuất cho Giám đốc Trung tâm công tác bảo đảm an toàn thông tin mạng định kỳ, hàng năm hoặc theo hướng dẫn của cơ quan chuyên môn.

c) Cử công chức tham gia hoạt động ứng cứu sự cố nhằm bảo đảm an toàn thông tin mạng khi có đề nghị từ các phòng, ban và trung tâm.

2. Các phòng, ban và Trung tâm trong phạm vi nhiệm vụ, quyền hạn của mình, có trách nhiệm phối hợp với Phòng Văn hóa - Xã hội, tổng hợp trong quá trình tham gia ứng cứu sự cố an toàn thông tin khi xảy ra sự cố.

3. Các phòng, ban và Trung tâm căn cứ chức năng, nhiệm vụ quyền hạn được giao phân công công chức của các phòng, ban và trung tâm thực hiện công tác đảm bảo an toàn, an ninh thông tin tại đơn vị.

III. BIỆN PHÁP THỰC HIỆN

1. Biện pháp phòng ngừa sự cố hệ thống thông tin:

1.1. Về thông tin, tuyên truyền:

- Tăng cường công tác tuyên truyền đến toàn thể các phòng, ban và trung tâm nâng cao ý thức trách nhiệm của cán bộ, công chức về đảm bảo an toàn thông tin trong hệ thống mạng LAN tại các phòng, ban và trung tâm.

- Nội dung tuyên truyền về an toàn, an ninh thông tin, gồm những điểm cơ bản, như sau:

+ Hệ thống thông tin là tập hợp các thiết bị viễn thông, công nghệ thông tin bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

+ An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

+ An ninh thông tin là việc bảo đảm thông tin trên mạng không gây phương hại đến an ninh quốc gia, trật tự an toàn xã hội, bí mật nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân.

+ Phần mềm độc hại là phần mềm có khả năng gây ra hoạt động không bình thường cho một phần hay toàn bộ hệ thống thông tin hoặc thực hiện sao chép, sửa đổi, xóa bỏ trái phép thông tin lưu trữ trong hệ thống thông tin.

+ Người dùng: Cán bộ, công chức tại các các phòng, ban và Trung tâm sử dụng máy tính, các thiết bị điện tử để xử lý công việc.

+ Tham số mạng: Là các tham số kỹ thuật được cài đặt trong các thiết bị mạng và thiết bị máy tính để tạo ra các địa chỉ kết nối trong mạng. Các máy tính gửi và nhận thông tin thông qua các địa chỉ kết nối này.

+ Tính toàn vẹn: Bảo vệ tính chính xác và tính đầy đủ của thông tin và các phương pháp xử lý thông tin.

+ Tính tin cậy: Đảm bảo thông tin chỉ có thể được truy cập bởi những người được cấp quyền sử dụng.

+ Tính sẵn sàng: Đảm bảo những người được cấp quyền có thể truy cập thông tin và các tài nguyên (mạng, máy chủ, tên miền, tài khoản thư điện tử, …) ngay khi có nhu cầu.

+ Sự cố an toàn thông tin mạng (viết tắt là sự cố) 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. Sự cố có thể là sự kiện đã, đang hoặc có khả năng xảy ra gây mất an toàn thông tin trên môi trường mạng (LAN, WAN, INTERNET, …), được phát hiện thông qua việc giám sát, đánh giá, phân tích của các cơ quan, tổ chức, cá nhân có liên quan hoặc được cảnh báo từ các chuyên gia, tổ chức về lĩnh vực an toàn thông tin trong nước và trên thế giới.

+ Sự cố có tính chất nghiêm trọng là sự cố có một hoặc nhiều tính chất sau: Có khả năng xảy ra trên diện rộng, lan nhanh; có khả năng phá hoại hệ thống mạng máy tính; lấy cắp dữ liệu, có thể gây thiệt hại lớn cho các hệ thống thông tin quan trọng như: Cổng thông tin điện tử, Cổng dịch vụ công và hệ thống thông tin Trung tâm Phục vụ hành chính công, hệ thống quản lý văn bản và điều hành, hệ thống thư điện tử công vụ.

+ Ứng phó sự cố 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.

+ Tuyên truyền, phổ biến các văn bản, quy định hiện hành về an toàn an ninh thông tin, như: Luật An toàn thông tin mạng; 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; 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; Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025; 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 hệ thống thông tin theo cấp độ; Quyết định số 03/2019/QĐ-UBND ngày 21/02/2019 của UBND tỉnh Quảng Ngãi về việc ban hành Quy chế bảo đảm an toàn, an ninh thông tin thuộc lĩnh vực công nghệ thông tin trong hoạt động của các cơ quan nhà nước trên địa bàn tỉnh Quảng Ngãi; Kế hoạch số 166/KH-UBND ngày 14/10/2022 của UBND tỉnh về tăng cường đảm bảo an toàn, an ninh thông tin trong hoạt động các cơ quan nhà nước tỉnh Quảng Ngãi đến năm 2025 và định hướng đến năm 2030 và các văn bản quy phạm pháp luật về

an toàn thông tin mạng và các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng.

1.2. Nhận diện các nguy cơ, sự cố hệ thống thông tin:

Các nguy cơ, sự cố có khả năng ảnh hưởng đến hệ thống thông tin đối với Hệ thống mạng LAN của các phòng, ban và Trung tâm, như sau:

1.2.1. Sự cố do bị tấn công mạng:

+ 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 từ chối dịch vụ;

+ Tấn công giả mạo;

+ 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.

1.2.2. 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.

1.2.3. 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 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.

1.2.4. Sự cố liên quan đến các thảm họa tự nhiên: Bão, lụt, động đất, hỏa hoạn,...

2. Phòng chống virus máy tính, bảo mật cơ sở dữ liệu và an ninh mạng:

a) Bảo mật số liệu: Cán bộ, công chức tại các phòng, ban và Trung tâm phải có trách nhiệm bảo mật số liệu nghiệp vụ trên máy tính. Tuyệt đối không chia sẻ thư mục, dữ liệu cá nhân trên hệ thống mạng LAN của các phòng, ban và Trung tâm.

b) Bảo mật truy cập: Các chương trình, phần mềm được bàn giao cho cán bộ, công chức sử dụng phải được thiết lập mật khẩu theo quy định. Kịp thời điều chỉnh vị trí công tác cho người sử dụng (khi có sự thay đổi); xóa khỏi hệ thống các tài khoản người dùng đã về hưu hoặc chuyển công tác.

c) Bảo mật hệ thống mạng và truyền tin: Mạng và đường truyền được áp dụng các chế độ bảo mật cần thiết, chống xâm nhập bất hợp pháp. Cán bộ, công chức có trách nhiệm thường xuyên theo dõi, kiểm tra phát hiện kịp thời các hoạt động xâm nhập vào máy tính và có biện pháp xử lý kịp thời.

d) An toàn trong sử dụng: Khi không làm việc với máy vi tính trong thời gian dài, Cán bộ, công chức tại các phòng, ban và Trung tâm phải tắt máy tính hoặc đặt chế độ bảo vệ để đảm bảo an toàn cho dữ liệu của cá nhân.

e) Phòng, chống virus: Cán bộ, công chức tại các phòng, ban và Trung tâm có trách nhiệm tuân thủ các biện pháp, tài liệu hướng dẫn về cảnh báo về lỗ hổng, cảnh báo nguy cơ tấn công theo tài liệu hướng dẫn của cơ quan có thẩm quyền nhằm rà soát, giám sát, ngăn chặn, phòng ngừa, xử lý kịp thời hạn chế đến mức thấp nhất nguy cơ gây mất an toàn an ninh thông tin. Mọi dữ liệu từ các thiết bị lưu trữ bên ngoài (USB, ổ cứng di động, thẻ nhớ, ...) đều phải được quét, diệt virus trước khi sao chép vào máy. Những máy tính phát hiện có virus phải được báo cáo ngay cho Phòng Văn hóa - Xã hội để có hướng xử lý, tránh tình trạng lây nhiễm sang các máy tính khác. Không truy cập vào các trang website, đường dẫn liên kết không rõ ràng; không truy cập vào các link hoặc tải về các file tài liệu từ các địa chỉ thư không nắm rõ thông tin, địa chỉ người gửi.

3. Kiểm soát việc cài đặt các phần mềm và thực hiện cơ chế sao lưu, phục hồi:

a) Kiểm soát chặt chẽ việc cài đặt các phần mềm mới lên máy chủ, máy trạm:

Các phần mềm được cài đặt trên máy chủ, máy trạm (*bao gồm hệ điều hành, các phần mềm ứng dụng văn phòng, phần mềm phục vụ công việc, tiện ích khác)* phải được thường xuyên theo dõi, cập nhật bản vá lỗi bảo mật của nhà phát triển, lựa chọn cài đặt các phần mềm chống, diệt virus, mã độc và thường xuyên cập nhật phiên bản mới, đặt lịch quét virus theo định kỳ.

b) Cơ chế sao lưu, phục hồi máy chủ, máy trạm:

Cán bộ, công chức tại các phòng, ban và trung tâm phải thực hiện việc sao lưu định kỳ cơ sở dữ liệu và các dữ liệu quan trọng khác (bao gồm dữ liệu phát sinh trong

quá trình vận hành các phần mềm ứng dụng như: các tập tin văn bản, hình ảnh, ...) vào các thiết bị lưu trữ bên ngoài (USB, ổ cứng di động, thẻ nhớ, …) nhằm phục vụ cho việc phục hồi, khắc phục dữ liệu kịp thời khi có sự cố xảy ra.

4. Đảm bảo an toàn hệ thống thông tin mạng LAN tại các phòng, ban và trung tâm:

a) Về cơ sở hạ tầng: Đảm bảo việc lắp đặt thiết bị chống sét, thiết bị cảnh báo phòng chống cháy, nổ tại trụ sở để bảo vệ hệ thống, thiết bị công nghệ thông tin.

b) Quản lý hệ thống mạng nội bộ: Các máy chủ, máy trạm trên hệ thống phải được cài đặt phần mềm diệt virus có bản quyền để kiểm soát, hạn chế việc truy cập trái phép từ bên ngoài.

c) Quản lý hệ thống mạng không dây (wifi): Khi thiết lập mạng không dây có kết nối vào mạng nội bộ phải thiết lập các thông số cần thiết như định danh, mật mã, mã hóa dữ liệu, có thay đổi mật mã định kỳ.

d) Quản lý truy cập từ xa vào mạng nội bộ: Đối với việc truy cập từ xa vào mạng nội bộ phải được theo dõi, quản lý chặt chẽ, nhất là truy cập có sử dụng chức năng quản trị, phải thiết lập mật mã độ an toàn cao, thường xuyên thay đổi mật mã, hạn chế truy cập từ xa vào mạng nội bộ từ các điểm truy cập Internet công cộng.

IV. PHÂN CÔNG THỰC HIỆN

1. Trách nhiệm của Trưởng các phòng chuyên môn, ban, trung tâm

- Thường xuyên chỉ đạo cán bộ, công chức của cơ quan, đơn vị mình thực hiện nghiêm các quy định bảo đảm an toàn thông tin hệ thống mạng LAN cơ quan.

- Phối hợp với Phòng Văn hóa - Xã hội xây dựng lực lượng trong công tác kiểm tra, phát hiện, xử lý kịp thời các sự cố về an toàn thông tin mạng.

2. Trách nhiệm của viên chức tại các phòng chuyên môn thuộc Trung tâm:

- Có trách nhiệm quản lý tài khoản, mật khẩu đăng nhập vào các phần mềm dùng chung được triển khai tại Các phòng, ban và trung tâm; thực hiện nghiêm các quy định về đảm bảo an toàn thông tin trong hệ thống mạng LAN cơ quan, Trung tâm. Thường xuyên thay đổi mật khẩu đủ mạnh (ít nhất 8 ký tự, có chữ hoa, chữ thường, số, ký tự đặc biệt) để đảm bảo an toàn, an ninh thông tin.

- Tự quản lý, bảo quản thiết bị công nghệ thông tin như: máy tính, máy in, máy scan, máy photocopy, ... mà mình được giao sử dụng; không tự ý thay đổi, tháo lắp thiết bị.

- Thực hiện tiếp nhận, xử lý, phát hành, quản lý và lưu trữ văn bản, hồ sơ điện tử trên phần mềm quản lý văn bản và điều hành (iOffice) đúng quy định trên môi trường mạng; thực hiện ký số văn bản điện tử cá nhân, đơn vị đảm bảo theo đúng quy

định pháp luật hiện hành. Không sử dụng gmail, yahoo, … để gửi, nhận văn bản giữa các cơ quan nhà nước.

- Không được tự ý cài đặt phần mềm download trên mạng khi chưa có sự đồng ý, hướng dẫn của Phòng Văn hóa - Xã hội và xây dựng lực lượng hoặc tự gỡ bỏ phần mềm diệt vius đã được cài đặt trên máy trạm.

- Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu, …), người sử dụng phải báo ngay cho Phòng Văn hóa - Xã hội để phối hợp xử lý kịp thời tránh lây lan đến các máy trạm khác.

3. Phương án ứng phó sự cố an toàn hệ thống thông tin:

Khi phát hiện ra bất kỳ dấu hiện nào liên quan đến việc bị nhiễm virus, nhiễm mã độc trên máy trạm (ví dụ: máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu, …), cán bộ, công chức tại các phòng, ban, trung tâm thực hiện các bước như sau:

+ ***Bước 1.*** Khoanh vùng cô lập sự cố:

- Sau khi phát hiện sự cố, cán bộ, công chức tại các phòng, ban, trung tâm thực hiện khoanh vùng cô lập máy tính bị sự cố, như: ngắt kết nối máy tính khỏi hệ thống thông tin mạng LAN của cơ quan (tắt máy, rút dây mạng, …).

- Báo cáo ngay Lãnh đạo phòng các dấu hiệu sự cố để phối hợp kiểm tra, xử lý.

+ ***Bước 2.*** Thu thập thông tin phục vụ phân tích sự cố:

- Phòng Văn hóa - Xã hội phối hợp với cán bộ, công chức tại các phòng, ban, trung tâm kiểm tra máy tính đang bị sự cố để nắm bắt thông tin ban đầu về sự cố.

- Các thông tin thu thập gồm: Thông tin hệ thống; chức năng của hệ thống; cấu hình của hệ thống (OS, servise, version, network, …); Thu thập chứng cứ; Thu thập bộ nhớ; Thu thập trạng thái network và các kết nối; Thu thập các tiến trình đang chạy; Thu thập hard drive media; Thu thập removeble media; Thu thập Log file, …).

+ ***Bước 3.*** Phân tích sự cố:

- Phòng Văn hóa - Xã hội phối hợp với các phòng, ban, trung tâm kiểm tra máy tính đang bị sự cố để phân tích nguyên nhân ban đầu về sự cố.

- Các thông tin phân tích gồm: Phân tích dòng thời gian; Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi; Thời gian thực hiện các cập nhật lớn đối với hệ thống; Thời điểm mà hệ thống sử dụng lần cuối cùng; Phân tích dữ liệu; Kiểm tra sự thay đổi cấu hình; Kiểm tra hệ thống tập tin có bị mã độc; Kiểm tra tập tin Internet history và các tập tin history khác; Kiểm tra Registry và tiến trình; Quan sát các tập tin, tiến trình lúc khởi động; Phân tích log file.

+ ***Bước 4.*** Xử lý sự cố:

- Trường hợp sự cố có khả năng kiểm soát, xử lý được: Cán bộ, công chức tại các phòng, ban, trung tâm tiến hành xử lý sự cố bao gồm các bước: Gỡ bỏ sự cố; Xác định và gỡ bỏ các backdoors; phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi; khôi phục dữ liệu; thu thập các tập tin, hình ảnh, email, … bị xóa, thời gian bị xóa; tìm kiếm các tập tin không thể khôi phục; khôi phục các tập tin phù hợp.

- Trường hợp sự cố ngoài khả năng kiểm soát, xử lý được (sự cố có tính chất nghiêm trọng): Triển khai ngay các biện pháp xử lý ngăn chặn tấn công tránh lây nhiễm sự cố các máy tính khác trên hệ thống thông tin và báo cáo Phòng Văn hóa - Xã hội đề xuất lãnh đạo UBND xã có văn bản đề nghị Sở Tư pháp, Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để có các biện pháp hỗ trợ, xử lý kịp thời.

+ ***Bước 5.*** Tổng hợp báo cáo:

- Sau khi triển khai các giải pháp ứng cứu sự cố, Phòng Văn hóa - Xã hội tham mưu trình Chủ tịch UBND xã tổ chức họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp ứng cứu cho các sự cố tương tự.

- Tham mưu Chủ tịch UBND xã gửi báo cáo kết quả ứng cứu sự cố xảy ra về Sở Tư pháp, Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để biết, theo dõi.

+ ***Bước 6.*** Lưu hồ sơ:

Toàn bộ các hồ sơ trong quá trình xử lý sự cố, Phòng Văn hóa – xã hội lưu trữ phục vụ các hoạt động quản lý và theo dõi, kiểm tra định kỳ.

V. TỔ CHỨC THỰC HIỆN

1. Các Phòng Kinh tế, Văn phòng HĐND&UBND, Trung tâm Phục vụ hành chính công, Trung tâm Cung ứng dịch vụ công trong phạm vi nhiệm vụ, quyền hạn của mình, có trách nhiệm phối hợp với Phòng Văn hóa - Xã hội trong quá trình tham gia ứng cứu sự cố an toàn thông tin khi xảy ra sự cố.

2. Các phòng, ban, trung tâm căn cứ chức năng, nhiệm vụ quyền hạn được giao phân công cán bộ, công chức tại phòng thực hiện công tác đảm bảo an toàn, an ninh thông tin.

3. Phương án này được phổ biến đến toàn thể cán bộ, công chức UBND xã biết để thực hiện. Trong quá trình thực hiện nếu có vướng mắc và cần sửa đổi, bổ sung, đề nghị các phòng, ban, trung tâm, đơn vị, cá nhân kịp thời phản ánh về Phòng Văn hóa - Xã hội để tổng hợp báo cáo Chủ tịch UBND xã xem xét, sửa đổi, bổ sung cho phù hợp./.