UỶ BAN NHÂN DÂN **XÃ YÊN THỌ**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨAVIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 06 /PA-UBND	*Yên Thọ, ngày 14 tháng 6 năm 2023*

PHƯƠNG ÁN
Ứng phó sự cố, đảm bảo an toàn thông tin mạng trên địa bàn xã Yên Thọ

Thực hiện Công văn số: 1303/UBND-VHTT ngày 29/5/2023 của UBND huyện Như Thanh về việc triển khai các nhiệm vụ bảo đảm an toàn thông tin mạng trên địa bàn huyện. UBND xã xây dựng Phương án Ứng cứu sự cố, đảm bảo an toàn thông tin mạng trên địa bàn xã cụ thể sau:

I. BẢO ĐẢM AN TOÀN, AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN CỦA UBND XÃ.

1. Hồ sơ, tài liệu quản lý

a) Lập hồ sơ, tài liệu hệ thống như tài liệu thiết kế, triển khai, quản trị, vận hành, bảo đảm an toàn thông tin.

b) Lưu trữ, bảo quản hồ sơ, tài liệu, xác định phạm vi phổ biến, sử dụng của tài liệu.

c) Thực hiện cập nhật tài liệu thường xuyên khi có thay đổi, xem xét định kỳ hàng năm.

2. Kiểm tra, đánh giá an toàn, an ninh mạng

a) Thực hiện kiểm tra, đánh giá chức năng và an toàn, an ninh mạng các hệ thống thông tin trước khi đưa vào sử dụng khi triển khai hệ thống mới hoặc nâng cấp hệ thống có thay đổi kiến trúc của hệ thống.

b) Thực hiện kiểm tra, đánh giá chức năng và an toàn, an ninh mạng trước khi đưa vào sử dụng đối với các phần mềm thuê khoán khi xây dựng phần mềm mới hoặc khi thay đổi phần mềm, thay đổi mã nguồn mà có ảnh hưởng đến kiến trúc của phần mềm

c) Chuẩn bị hồ sơ, thực hiện các bước, quy trình kiểm tra, đánh giá an toàn, an ninh mạng theo quy định, quy trình, hướng dẫn của Tổ ứng cứu sự cố huyện; của đơn vị chuyên trách an toàn, an ninh mạng của Trung Tâm CNTT tỉnh Thanh Hóa.

3. Giám sát an toàn, an ninh mạng

a) Triển khai giám sát 24/7 đối với các hệ thống thông tin

b) Các yêu cầu giám sát cơ bản gồm: trạng thái hoạt động up/down; lưu lượng mạng, dịch vụ. Ngoài ra, thực hiện giám sát an toàn thông tin theo hướng dẫn tại Thông tư số 31/2017/TT-BTTTT. Tùy vào điều kiện, nguồn lực và mức độ quan trọng của các hệ thống thông tin, có thể triển khai thêm các phương án giám sát khác để giám sát bất thường, nguy cơ, rủi ro hoặc dấu hiệu an toàn, an ninh mạng của hệ thống thông tin.

c) Xây dựng các quy trình xử lý đối với các sự cố an toàn, an ninh mạng được phát hiện qua công tác giám sát. Đối với các sự cố chưa có trong quy trình, có khả năng ảnh hưởng nguy hiểm tới các hệ thống thông tin quan trọng thì thực hiện cung cấp thông tin kịp thời cho Tổ ứng cứu sự cố của huyện; đơn vị chuyên trách an toàn, an ninh mạng của tỉnh Thanh Hóa để phối hợp điều tra, phân tích và xử lý.

d) Thực hiện báo cáo định kỳ, báo cáo khi có sự cố xảy ra hoặc báo cáo đột xuất theo yêu cầu của các cấp có thẩm quyền.

4. Quản lý rủi ro

a) Thực hiện đánh giá rủi ro đối với các hệ thống thông tin.

b) Nội dung đánh giá rủi ro tập trung xác định các điểm yếu, mối đe dọa đối với tài sản của các hệ thống thông tin, từ đó xác định hậu quả và mức độ ảnh hưởng. Đồng thời đưa ra biện pháp để xử lý rủi ro bảo đảm cân đối giữa nguồn lực và giá trị mang lại.

5. Kết thúc vận hành, khai thác, sửa chữa, thanh lý, hủy bỏ

a) Thực hiện hủy bỏ toàn bộ thông tin, dữ liệu trên hệ thống với sự xác nhận của đơn vị chủ quản hệ thống thông tin khi kết thúc vận hành, khai thác, thanh lý, hủy bỏ hệ thống thông tin. Trong trường hợp thông tin, dữ liệu của hệ thống thông tin lưu trữ trên tài sản vật lý, đơn vị chủ quản hệ thống thông tin thực hiện các biện pháp tiêu hủy hoặc xóa thông tin bảo đảm không có khả năng phục hồi. Với trường hợp đặc biệt không thể tiêu hủy được thông tin, dữ liệu thì sử dụng biện pháp tiêu hủy cấu trúc phần lưu trữ dữ liệu trên tài sản đó.

b) Đối với các hệ thống thông tin có dữ liệu được lưu trữ trên tài sản vật lý cần phải mang đi bảo hành, bảo dưỡng, sửa chữa bên ngoài thì phải được sự phê duyệt của cấp có thẩm quyền và thực hiện các biện pháp bảo vệ dữ liệu; có cam kết bảo mật thông tin giữa bên có dữ liệu và bên cung cấp dịch vụ dịch vụ sửa chữa thiết bị lưu trữ dữ liệu.

II. PHƯƠNG ÁN ỨNG PHÓ, KHẮC PHỤC SỰ CỐ AN TOÀN, ÁN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN CỦA UBND XÃ.

1. Nguyên tắc thực hiện

Phương án ứng phó, khắc phục sự cố an toàn, an ninh mạng được thực hiện theo nguyên tắc: Phát hiện hoặc tiếp nhận sự cố; xác minh, phân tích, đánh giá và phân loại sự cố; quyết định lựa chọn phương án và phối hợp các đơn vị liên quan; ứng cứu sự cố, khôi phục hệ thống; Điều phối, ứng cứu sự cố; kết thúc sự cố; Khắc phục, phòng ngừa sự cố tái diễn; Hỗ trợ sau sự cố.

2. Phát hiện, tiếp nhận, ứng cứu ban đầu và thông báo sự cố

a) Thực hiện đánh giá, xác định nguy cơ, sự cố an toàn, an ninh mạng trong hoạt động quản trị, vận hành các hệ thống thông tin.

b) Đơn vị, cá nhân vận hành hệ thống thông tin chủ trì, phối hợp với Tổ ứng cứu sự cố của xã và các cơ quan, tổ chức liên quan tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài (cảnh báo sự cố: Văn bản, email, điện thoại, website, mạng xã hội...; phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá). Khi xác định được sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập

chứng cứ, xác định nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp.

Các loại sự cố chính, bao gồm:

- Sự cố do bị tấn công hệ thống mạng;

- Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền...;

- Sự cố do lỗi của người quản trị, vận hành hệ thống;

- Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn,...

c) Triển khai, lựa chọn các bước ưu tiên ứng cứu ban đầu:

Sau khi đã xác định sự cố xảy ra, đơn vị, cá nhân vận hành hệ thống thông tin tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo phương án đối phó, ứng cứu một số tình huống sự cố cụ thể hoặc theo tư vấn, hướng dẫn của Đơn vị thường trực về ứng cứu sự cố của huyện.

d) Thông báo, báo cáo sự cố:

Sau khi triển khai các bước ưu tiên ứng cứu ban đầu, đơn vị, cá nhân vận hành hệ thống thông tin tổ chức thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan, tổ chức theo quy định; cụ thể:

- Thông báo sự cố tới Tổ ứng cứu sự cố của xã chậm nhất 03 ngày kể từ khi phát hiện sự cố; trường hợp xác định sự cố có thể vượt khả năng xử lý, đội ứng cứu sự cố của xã thực hiện báo cáo ban đầu sự cố bằng văn bản về đơn vị thường trực về ứng cứu sự cố của huyện.

đ) Điều phối công tác ứng cứu

- Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của Bộ phận vận hành hệ thống thông tin, Tổ ứng cứu sự cố của xã thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ứng cứu sự cố.

- Trường hợp sự cố vượt quá khả năng ứng cứu của Đội ứng cứu sự cố cấp xã thực hiện báo cáo về Tổ ứng cứu sự cố của huyện để đề nghị điều phối ứng cứu sự cố.

3. Triển khai ứng cứu, ngăn chặn sự cố

Đơn vị, cá nhân vận hành hệ thống phối hợp với Tổ ứng cứu sự cố của xã và các đơn vị liên quan tiến hành triển khai theo phương án đối phó, ứng cứu một số tình huống sự cố cụ thể. Trong đó, tập trung nguồn lực thực hiện:

a) Triển khai thu thập chứng cứ, xác định phạm vi, đối tượng bị ảnh hưởng.

- Thu thập thông tin ban đầu để phục vụ phân tích sự cố:

+ Thông tin về đầu mối liên hệ;

+ Thu thập thông tin hệ thống;

+ Thu thập chức năng của hệ thống;

+ Thu thập 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 log file;

+ Thu thập các cổng đang mở của hệ thống.

b) Triển khai phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

- Phân tích sự cố, xác định nguồn gốc tấn công

+ 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

+ Phân tích hệ thống quản lý tệp (File System)

+ Phân tích Resgitry

+ Phân tích Windows

+ Phân tích kết nối mạng

4. Xử lý sự cố, gỡ bỏ và khôi phục

a) Xử lý sự cố, gỡ bỏ

Sau khi đã triển khai ngăn chặn sự cố, Bộ phận vận hành hệ thống thông tin, tổ ứng cứu sự cố và các cá nhân có liên quan triển khai tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

b) Khôi phục

Bộ phận vận hành hệ thống chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục hệ thống thông tin dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng phần mềm bảo đảm an toàn thông tin cho hệ thống thông tin.

c) Kiểm tra, đánh giá hệ thống thông tin

Bộ phận vận hành hệ thống và các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức các bước tương ứng để xử lý dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.

4. Tổng kết, đánh giá

a) Tổng kết, đúc rút kinh nghiệm:

Bộ phận vận hành hệ thống thông tin bị sự cố phối hợp với Tổ ứng cứu sự cố của xã triển khai tổng hợp tất cả các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai, báo cáo Cơ quan chuyên trách về an toàn thông tin của huyện; tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai...

b) Xây dựng báo cáo kết thúc ứng phó sự cố:

Bộ phận vận hành hệ thống thông tin bị sự cố, Tổ ứng cứu sự cố xã triển khai tổng hợp và xây dựng báo cáo kết thúc ứng phó sự cố, trong đó trình bày chi tiết quá trình xử lý sự cố, tóm tắt tổng quát về tình hình sự cố và đề xuất cách thức triển khai điều phối, ứng cứu sự cố nhằm xử lý nhanh, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự.

Sau khi kết thúc ứng cứu sự cố, trong vòng 10 ngày Tổ ứng cứu sự cố phải xây dựng báo cáo kết thúc ứng phó sự cố, gửi về Tổ ứng cứu sự cố về an toàn thông tin của huyện khi có yêu cầu./.

***Nơi nhận*:**
- Phòng VH&TT;
- TTr Đảng ủy - HĐND xã;
- Chủ tịch, các PCT UBND xã;
- Tổ ứng cứu ATTT mạng;
- Lưu: VP,VH;

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Nguyễn Hữu Đại