ỦY BAN NHÂN DÂN **XÃ PHỔ AN**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 274 /QĐ-UBND	*Phổ An, ngày 07 tháng 11 năm 2024*

QUYẾT ĐỊNH

Về việc ban hành Phương án Ứng phó sự cố, đảm bảo an toàn thông tin đối với Hệ thống mạng nội bộ của Uỷ ban nhân dân xã Phổ An

CHỦ TỊCH ỦY BAN NHÂN DÂN XÃ PHỔ AN

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006; Căn

cứ Luật an toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

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 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP của Chính phủ;

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

Căn cứ Quyết định số 3810/QĐ-UBND ngày 25/10/2024 của Chủ tịch UBND thị xã Đức Phổ về việc phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống mạng nội bộ của UBND xã Phổ An;

Theo đề nghị của công chức Văn phòng - Thống kê xã.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Phương án Ứng phó sự cố, đảm bảo an toàn thông tin đối với Hệ thống mạng nội bộ của Uỷ ban nhân dân xã Phổ An

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

Điều 3. Văn phòng - Thống kê xã, các bộ phận chuyên môn, các hội, đoàn thể và các cơ quan, đơn vị có liên quan chịu thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- Phòng Văn hóa & Thông tin thị xã;
- TT Đảng ủy, HĐND xã;
- CT, các PCT UBND xã;
- Lưu: VT.

CHỦ TỊCH

Nguyễn Minh Hà

PHƯƠNG ÁN
Ứng phó sự cố, đảm bảo an toàn thông tin đối với Hệ thống mạng nội bộ của Uỷ ban nhân dân xã Phổ An

(Ban hành kèm theo Quyết định số: ……/QĐ-UBND, ngày …../11/2024 của Chủ tịch UBND xã Phổ An)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

1. Quy chế này quy định các các biện pháp nhằm ứng phó sự cố, bảo đảm an toàn thông tin cho các Hệ thống thông tin nội bộ của UBND xã Phổ An *(sau đây gọi tắt là các Hệ thống thông tin)*.

2. Đối tượng áp dụng

a) Các bộ phận, cán bộ, công chức, người lao động thuộc UBND xã Phổ An

b) Cơ quan, tổ chức, cá nhân liên quan đến hoạt động ứng phó sự cố đảm bảo an toàn thông tin.

Điều 2 . 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 (sau đây gọi tắt là sự cố).

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 1 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 1.

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

3. Ứng phó 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.

Điều 3. Nguyên tắc ứng phó sự cố

1. Tuân thủ các quy định pháp luật về điều phối, ứng phó sự cố an toàn thông tin mạng.

2. Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

3. Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các bộ phận.

4. Ứng phó sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

Chương III

PHƯƠNG ÁN ỨNG PHÓ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 4. Các nguy cơ mất an toàn thông tin

- Nguy cơ mất an toàn thông tin về khía cạnh vật lý: Nguy cơ mất an toàn thông tin về khía cạnh vật lý là nguy cơ do mất điện, nhiệt độ, độ ẩm không đảm bảo, hỏa hoạn, thiên tai, thiết bị phần cứng bị hư hỏng, phá hoại.

- Nguy cơ bị mất, hỏng, sửa đổi nội dung thông tin: Người dùng có thể vô tình để lộ mật khẩu hoặc không thao tác đúng quy trình tạo cơ hội cho kẻ xấu lợi dụng để lấy cắp hoặc làm hỏng thông tin. Kẻ xấu có thể sử dụng công cụ hoặc kỹ thuật của mình để thay đổi nội dung thông tin (các file) nhằm sai lệnh thông tin của chủ sở hữu hợp pháp.

- Nguy cơ bị tấn công bởi các phần mềm độc hại: Các phần mềm độc hại tấn công bằng nhiều phương pháp khác nhau để xâm nhập vào hệ thống với các mục đích khác nhau như: virus, sâu máy tính (Worm), phần mềm gián điệp (Spyware),...

- Nguy cơ xâm nhập từ lỗ hổng bảo mật: 3 Lỗ hổng bảo mật thường là do lỗi lập trình, lỗi hoặc sự cố phần mềm, nằm trong một hoặc nhiều thành phần tạo nên hệ điều hành hoặc trong chương trình cài đặt trên máy tính.

- Nguy cơ xâm nhập do bị tấn công bằng cách phá mật khẩu: Quá trình truy cập vào một hệ điều hành có thể được bảo vệ bằng một khoản mục người dùng và một mật khẩu. Đôi khi người dùng khoản mục lại làm mất đi mục đích bảo vệ của nó bằng cách chia sẻ mật khẩu với những người khác, ghi mật khẩu ra và để nó công khai hoặc để ở một nơi nào đó cho dễ tìm trong khu vực làm việc của mình.

- Nguy cơ mất an toàn thông tin do sử dụng e-mail: Tấn công có chủ đích bằng thư điện tử là tấn công bằng thư điện tử giả mạo giống như thư điện tử được gửi từ người quen, có thể gắn tập tin đính kèm nhằm làm cho thiết bị bị nhiễm virus. Cách thức tấn công này thường nhằm vào một cá nhân hay một tổ chức cụ thể. Thư điện tử đính kèm tập tin chứa virus được gửi từ kẻ mạo danh là một đồng nghiệp hoặc một đối tác nào đó. Người dùng bị tấn công bằng thư điện tử có thể bị đánh cắp mật khẩu hoặc bị lây nhiễm virus. Ngoài ra, e-mail cũng có thể chứa một liên kết tới một web site giả.

- Nguy cơ mất an toàn thông tin trong quá trình truyền tin: Trong quá trình lưu thông và giao dịch thông tin trên mạng internet nguy cơ mất an toàn thông tin trong quá trình truyền tin là rất cao do kẻ xấu chặn đường truyền và thay đổi hoặc phá hỏng nội dung thông tin rồi gửi tiếp tục đến người nhận.

Điều 5. Điều phối công tác ứng cứu

- Căn cứ vào tính chất sự cố, công chức phụ trách an toàn thông tin của UBND xã (Văn phòng - Thống kê) 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 UBND xã thì thực hiện báo cáo về phòng cho Phòng Văn hóa và Thông tin thị xã Đức Phổ và quản trị mạng của UBND thị xã để có biện pháp điều phối ứng cứu sự cố.

Điều 6. Quy trình ứng cứu sự cố an toàn thông tin mạng

Khi phát hiện ra bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm virus, nhiễm mã độc (ví dụ: Máy hoạt động chậm bất thường, cảnh báo từ phần mềm diệt virus, mất dữ liệu,…), người dùng thực hiện các bước như sau:

- *Bước 1*. Khoanh vùng cô lập sự cố

+ Sau khi phát hiện sự cố, người dùng thực hiện cô lập máy tính bị sự cố, như: Ngắt kết nối máy tính khỏi hệ thống thông tin mạng nội bộ của UBND xã (tắt máy, rút dây mạng…).

+ Báo ngay cho công chức Văn phòng - Thống kê các dấu hiệu sự cố để báo cáo kịp thời cho Phòng Văn hóa và Thông tin và quản trị mạng của UBND thị xã (bộ phận ứng cứu).

- *Bước 2*. Thu thập thông tin 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

- *Bước 3*. Phân tích sự cố, 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 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.

- *Bước 4.* Xử lý sự cố

+ Sau khi đã triển khai ngăn chặn sự cố, bộ phận 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.

+ 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.

+ 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.

- *Bước 5*. Tổng hợp báo cáo

Sau khi triển khai các giải pháp ứng cứu sự cố, công chức Văn phòng - Thống kê tham mưu 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, đồng thời gửi báo cáo kết quả ứng cứu sự cố xảy ra về Phòng Văn hoá - Thông tin thị xã và Sở Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Quảng Ngãi để biết, theo dõi (Toàn bộ các hồ sơ trong quá trình xử lý sự cố, công chức phụ trách an toàn thông tin UBND xã có trách nhiệm lưu trữ phục vụ các hoạt động quản lý và theo dõi, kiểm tra định kỳ về công tác chuyển đổi số của xã).

Chương VI

TỔ CHỨC THỰC HIỆN

Điều 7. Trách nhiệm của cán bộ, công chức, người lao động thuộc UBND xã Phổ An

+ Nghiêm túc chấp hành các quy chế, quy trình nội bộ và các quy định khác của pháp luật về an toàn thông tin mạng.

+ Tự quản lý, bảo quản thiết bị, tài khoản, ứng dụng mà mình được giao sử dụng; khai thác, sử dụng có hiệu quả các phần mềm dùng chung của tỉnh.

+ Tìm kiếm thông tin trên mạng từ các trang chính thống và tìm kiếm văn bản trên liên quan đến công tác tham mưu thuộc lĩnh vực mình tại Cổng

Thông tin điện tử UBND tỉnh và Cổng Thông tin điện tử thị xã, Trang Thông tin điện tử xã.

+ Phối hợp với công chức Văn phòng - Thống kê và quản trị mạng trong việc kiểm soát, phát hiện và khắc phục các sự cố an toàn thông tin mạng.

Điều 8. Trách nhiệm của công chức Văn phòng - Thống kê

+ Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trong nội bộ cơ quan.

+ Tùy theo mức độ sự cố, phối hợp với Phòng Văn hoá - Thông tin và Quản trị mạng của UBND thị xã để xử lý, ứng cứu các sự cố an toàn thông tin mạng.

+ Tổng hợp và báo cáo về tình hình an toàn thông tin mạng theo định kỳ của Sở Thông tin và Truyền thông.

+ Tham gia các chương trình đào tạo, tập huấn về công tác bảo đảm an toàn thông tin mạng do Sở Thông tin và Truyền thông tổ chức.

+ Tham mưu Chủ tịch UBND xã đôn đốc, chỉ đạo các cá nhân thực hiện nghiêm túc, đảm bảo an toàn, an ninh thông tin; tuyên truyền hướng dẫn đến cán bộ, công chức, viên chức và người lao động trong các cơ quan, đơn vị trên địa bàn về công tác bảo đảm an toàn thông tin mạng.

- Xây dựng kế hoạch nâng cấp, bảo trì, sửa chữa, cài đặt phần mềm Phòng chống mã độc ... Đề xuất sửa chữa, nâng cấp, thay thế trang thiết bị không phù hợp để đảm bảo an toàn thông tin trong toàn hệ thống./.