UỶ BAN NHÂN DÂN **HUYỆN NGUYÊN BÌNH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập – Tự do – Hạnh Phúc**
Số: 272 /KH-UBND	*Nguyên Bình, ngày 30 tháng 12 năm 2022*

KỊCH BẢN
Phương án phối hợp ứng cứu sự cố an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của Ủy ban nhân dân huyện Nguyên Bình

Thực hiện Công văn số 2917/UBND-VX ngày 10 tháng 11 năm 2022 của Ủy ban nhân dân tỉnh Cao Bằng về việc thực hiện 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;

Ủy ban nhân dân huyện Nguyên Bình xây dựng kịch bản phương án ứng cứu sự cố cho hệ thống thông tin cụ thể như sau:

CHƯƠNG I
CÁC QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng.

- Kịch bản này quy định phương án phối hợp ứng cứu sự cố an toàn thông tin mạng trong hoạt động hoạt động ứng dụng công nghệ thông tin (CNTT).

- Kịch bản này được áp dụng đối với các Phòng, ban trực thuộc Ủy ban nhân dân (UBND) huyện.

Điều 2. Nguyên tắc, phương châm ứng cứu sự cố

Phân nhóm sự cố an toàn thông tin (ATTT) mạng đáp ứng các tiêu chí sau:

- Hệ thống thông tin bị một số trong 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 đảm bảo tính toàn vẹn và không có khả năng phục hồi.

+ 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.

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

Điều 3. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các lực lượng ứng phó sự cố

1. Văn phòng HĐND&UBND, Phòng Văn hóa và Thông tin là bộ phận phụ trách ứng cứu sự cố ATTT mạng có trách nhiệm:

- Tham gia hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng nội bộ khi có yêu cầu.

- Phối hợp với Sở Thông tin và Truyền thông tin, Công an huyện và các đơn vị liên quan trong việc tăng cường tập trung phát hiện, cảnh báo sớm các nguy cơ mất ATTT mạng, nhanh chóng khắc phục, phục hồi hệ thống khi xảy ra sự cố.

- Tham gia đầy đủ các khóa đào tạo, tập huấn, nâng cao về ATTT mạng do cấp trên tổ chức.

2. Các Phòng, ban, ngành, Ủy ban nhân dân các xã, thị trấn có trách nhiệm:

- Kiểm tra, rà soát hệ thống thông tin khi có cảnh báo, thống báo về các nguy cơ mất ATTT mạng từ các cơ quan chức năng.

- Cử các cán bộ, công chức, viên chức phụ trách ATTT mạng tham gia ứng cứu sự cố ATTT khi xảy ra sự cố.

- Tuyên truyền, phổ biến đến toàn thể cán bộ, công chức, viên chức về tầm quan trọng của việc đảm bảo ATTT mạng.

- Tham gia đầy đủ các khóa đào tạo, tập huấn, bồi dưỡng về ATTT mạng.

CHƯƠNG II

ĐÁNH GIÁ NGUY CƠ, SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 4. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng.

1. Đánh giá hiện trạng và khả năng bảo đảm ATTT mạng của hệ thống thông tin và các đối tượng cần bảo vệ.

2. Đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ.

3. Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố.

4. Đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

CHƯƠNG III

PHƯƠNG ÁN ĐỐI PHÓ, ỨNG CỨU SỰ CỐ ĐỐI VỚI MỘT SỐ TÌNH HUỐNG SỰ CỐ CỤ THỂ

Điều 5. Tiêu chí xây dựng phương án đối phó, ứng cứu sự cố ATTT mạng

Phương án đối phó, ứng cứu sự cố ATTT mạng phải đặt ra các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi

sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

1. Phương pháp, cách thức để xác định nhanh chóng, kịp thời, nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp:

- Sự cố do bị tấn công mạng;

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

- 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…

2. Phương án đối phó, ứng cứu, khắc phục sự cố đối với một hoặc nhiều tính huống sau:

* Tình huống 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.

* Tình huống sự cố do lỗi 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;

- Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuaath.

* Tình huống 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.

* Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn…

3. Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, giữa các đơn vị trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố.

CHƯƠNG IV

TRIỂN KHAI PHÒNG NGỪA SỰ CỐ, GIÁM SÁT PHÁT HIỆN, BẢO ĐẢM CÁC ĐIỀU KIỆN SẴN SÀNG ĐỐI PHÓ, ỨNG CỨU, KHẮC PHỤC SỰ CỐ

Điều 6. Thực hiện xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố.

1. Các nội dung, nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm:

- Thực hiện nghiêm công tác giám sát, phát hiện sớm nguy cơ, sụp đổ.

- Kiểm tra, đánh giá ATTT mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc.

- Phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro an toàn thông tin mạng, phần mềm độc hại.

- Xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

2. Các nội dung, nhiệm vụ nhằm đảm bảo các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố:

- Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ ứng cứu, khắc phục sự cố; thuê dịch vụ bảo đảm an toàn thông tin.

- Chuẩn bị các nguồn lực để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra.

- Tham gia các hoạt động của mạng lưới ứng cứu sự cố.

CHƯƠNG V

TỔ CHỨC THỰC HIỆN

Điều 7. Trách nhiệm của Văn phòng HĐND&UBND, Phòng Văn hóa và Thông tin.

1. Chủ trì, phối hợp với các cơ quan, đơn vị ban hành kịch bản, phương án cụ thể thực hiện các nội dung của kịch bản này.

2. Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các dự cố về ATTT mạng.

3. Chủ trì, phối hợp với các cơ quan, đơn vị tiến hành kiểm tra các công tác bảo đảm ATTT mạnh định kỳ hàng năm hoặc theo hướng dẫn của cơ quan chuyên môn.

Điều 8. Trách nhiệm của Phòng Tài chính- Kế hoạch

Thực hiện cân đối ngân sách, tham mưu bố trí ngồn kinh phí tổ chức ứng cứu và thực hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố vào các hoạch về đảm bảo ATTT mạng, ứng dụng CNTT.

Điều 9. Trách nhiệm của các phòng, ban, ngành, Ủy ban nhân dân các xã, thị trấn

1. Căn cứ chức năng, nhiệm vụ được giao chủ động tổ chức, triển khai, thực hiện và xây dựng kịch bản, phương án phối hợp ứng phó ATTT mạng trong hoạt động ứng dụng CNTT tại đơn vị.

2. Quan tâm, chú trọng đến công tác bảo đảm ATTT mạng cho hệ thống tại đơn vị.

3. Phối hợp với các cơ quan, đơn vị liên quan thực hiện công tác ứng phó khi có sự cố ATTT mạng tại đơn vị.

4. Tổ chức quán triệt và triển khai kịch bản này đến toàn thể cán bộ, công chức, viên chức và người lao động.

Điều 10. Trong quá trình thực hiện nếu có vấn đề vướng mắc, phát sinh, các đơn vị kịp thời phản ánh về Ủy ban nhân dân huyện (qua Phòng Văn hóa và Thông tin hoặc Văn phòng HĐND và UBND huyện) để tổng hợp báo cáo Sở Thông tin và Truyền thông theo quy định./.

Nơi nhận:
- Sở Thông tin và Truyền thông;
- CT, các PCT UBND huyện;
- Các phòng, ban, ngành thuộc UBND huyện;
- UBND các xã, thị trấn;
- Trang TTĐT huyện;
- Lưu VT.

TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Dương Hiển Hòa