UỶ BAN NHÂN DÂN **XÃ KIẾN MINH**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 456/QĐ-UBND	*Kiến Minh, ngày 21 tháng 04 năm 2026*

QUYẾT ĐỊNH
Về việc ban hành phương án, kịch bản ứng cứu sự cố hệ thống thông tin xã Kiến Minh

UỶ BAN NHÂN DÂN XÃ KIẾN MINH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 16/6/2025;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

Căn cứ Văn bản hợp nhất số 27/VBHN-VPQH ngày 02/8/2023 của Văn phòng Quốc hội về Luật Công nghệ thông tin;

Căn cứ 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;

Căn cứ Nghị định số 42/2022/NĐ-CP ngày 24/6/2022 của Chính phủ quy định về việc cung cấp thông tin và dịch vụ công trực tuyến của cơ quan nhà nước trên môi trường mạng;

Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ Quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

Căn cứ Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ các Thông tư của Bộ Thông tin và Truyền thông: số 11/2015/TT-BTTTT ngày 05/5/2015 quy định Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp; số 20/2017/TT-BTTTT ngày 12/9/2017 quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; số 17/2021/TT-BTTTT ngày 30/11/2021 về việc sửa đổi, bổ sung một số điều Thông tư số 11/2015/TT-BTTTT ngày 05/5/2015 của Bộ Thông tin và Truyền thông Quy định Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp; số 12/2022/TT-BTTTT ngày 12/8/2022

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;

Theo đề nghị của Chánh văn phòng HĐND và UBND xã..

QUYẾT ĐỊNH:

Điều 1. Ban hành theo Quyết định này phương án, kịch bản ứng cứu sự cố hệ thống thông tin tại Đảng uỷ, Hội động nhân dân và Uỷ ban nhân dân xã Kiến Minh.

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

Điều 3. Chánh Văn phòng HĐND và UBND xã, Trưởng các phòng, cơ quan, đơn vị, công chức, viên chức, người lao động thuộc xã Kiến Minh và các cá nhân liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Công an thành phố; (để b/c);
- TT ĐU;
- TT HĐND xã;
- CT, các PCT UBND xã;
- UB MTTQ VN xã và các tổ chức CT - XH;
- Các phòng chuyên môn;
- Như điều 3;
- Lưu: VT.

TM. UỶ BAN NHÂN DÂN
CHỦ TỊCH

U.B.N.D XÃ KIẾN MINH T.P HẢI PHÒNG

Phạm Tiến Thuật

PHƯƠNG ÁN, KỊCH BẢN ỨNG CỨU
SỰ CỐ HỆ THỐNG THÔNG TIN XÃ KIẾN MINH

(Ban hành kèm theo Quyết định số 456/QĐ-UBND ngày 21 tháng 04 năm 2026 của Uỷ ban nhân dân xã Kiến Minh)

CHƯƠNG I
CÁC QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Phạm vi điều chỉnh: Phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin trong hoạt động ứng dụng công nghệ thông tin, chuyển đổi số của xã Kiến Minh.

2. Đối tượng áp dụng: Các phòng, cơ quan, đơn vị, cán bộ, công chức, viên chức, người lao động thuộc quản lý của Đảng uỷ, Hội đồng nhân dân và Uỷ ban nhân dân xã Kiến Minh.

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

1. Tuân thủ các quy định pháp luật về điều phối, ứng cứu 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 phòng ban.

4. Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của Văn phòng HĐND và UBND cùng Tổ chuyên trách an toàn thông tin.

5. Thông tin trao đổi giữa các phòng ban trong đơn vị phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

6. Bảo đảm bí mật thông tin biết được khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của Uỷ ban nhân dân.

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

Văn phòng HĐND và UBND là cơ quan chuyên trách ứng cứu sự cố ATTT mạng của xã có trách nhiệm: Tham gia hoạt động ứng cứu khẩn cấp bảo đảm ATTT mạng nội bộ khi có yêu cầu từ các phòng, đơn vị trực thuộc xã.

Các phòng, đơn vị trực thuộc có trách nhiệm cử cán bộ, công chức phụ trách ATTT tham gia ứng cứu sự cố ATTT khi xảy ra sự cố.

CHƯƠNG II
ĐÁNH GIÁ CÁC 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 các 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).

5. 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: 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 website 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.

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 an toàn thông tin 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 tình huống sau:

a) 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.

b) Tình huống 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;

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

c) 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.

d) Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn v.v....

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

Điều 6. Quy trình ứng cứu sự cố ATTT mạng

Bước 1: Thông báo sự cố

Cán bộ công chức, viên chức, người lao động tại các phòng, ban, đơn vị thuộc xã khi gặp sự cố trong quá trình sử dụng máy tính có kết nối mạng thực hiện thông báo ngay cho Văn phòng HĐND và UBND và Tổ chuyên trách an toàn thông tin.

Bước 2: Tiếp nhận sự cố

Văn phòng HĐND và UBND tiếp nhận thông tin về sự cố qua các phương thức: điện thoại, trực tiếp, ...

Bước 3: Xác minh/xác nhận sự cố

Văn phòng HĐND và UBND triển khai tiến hành xác minh/xác nhận sự cố

bao gồm các thông tin như sau:

- Tình trạng (Sự cố sẽ xảy ra; Sự cố đang xảy ra; Sự cố đã xảy ra);

- Mức độ (Sự cố nghiêm trọng; Sự cố bình thường);

- Phạm vi (Sự cố diện rộng; Sự cố mạng máy tính; Sự cố một máy tính);

- Và địa điểm xảy ra sự cố.

Bước 4: Phân loại sự cố

Văn phòng HĐND và UBND thực hiện phân loại sự cố theo điều Điều 5 kịch bản này

Bước 5: Báo cáo lãnh đạo, xin ý kiến chỉ đạo

Ngay sau khi phân loại được sự cố Văn phòng HĐND và UBND có trách nhiệm báo cáo Lãnh đạo đơn vị để xem xét loại sự cố và tuỳ theo đối tượng sẽ tiến hành xử lý.

Trường hợp sự cố được phân loại thông thường thì Văn phòng HĐND và UBND báo cho các bên liên quan để tiếp tục triển khai theo phương án ứng cứu sự cố an toàn thông tin mạng thông thường theo quy trình tại Phụ lục I (Trích Quy trình ứng cứu sự cố thông thường của Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017); báo cáo sự cố đến Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hải Phòng (qua Phòng An ninh mạng và phòng, chống tội phạm công nghệ cao Công an thành phố Hải Phòng) để phối hợp xử lý.

Trường hợp sự cố được phân loại nghiêm trọng thì gửi báo cáo sự cố đến Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hải Phòng (qua Phòng An ninh mạng và phòng, chống tội phạm công nghệ cao Công an thành phố Hải Phòng) về sự cố nghiêm trọng để có phương án ứng cứu; và tổ chức ứng cứu, xử lý sự cố: các đơn vị tham gia lực lượng ứng cứu; nguồn lực cần thiết để ứng cứu sự cố; dự kiến triệu tập bộ phận tác nghiệp ứng cứu khẩn cấp và thực hiện tiếp các bước tiếp theo quy định tại Điều 14 Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

Bước 6: Phối hợp với Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hải Phòng

Thu thập thông tin phục vụ phân tích sự cố; Phân tích sự cố; Xử lý sự cố; Khôi phục, kiểm tra, báo cáo, tổng kết, đánh giá.

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 7. 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, nội dung bao gồm:

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, sự cố.

- 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 bảo đảm 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 8. Trách nhiệm của Văn phòng HĐND và UBND

- Chủ trì, phối hợp với các phòng, đơn vị trực thuộc ban hành kế hoạch, phương án cụ thể thực hiện các nội dung tại Điều 4 và Điều 5, Điều 6, Điều 7 của Kịch bản này.

- Làm đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về ATTT mạng trong hoạt động của cơ quan.

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

- Tham mưu đưa nội dung dự phòng kinh phí, nhân lực, vật lực thường trực sẵn sàng ứng cứu sự cố; triển khai điều hành phối hợp tổ chức ứng cứu và thực

hiện ứng cứu, xử lý, ngăn chặn, khắc phục sự cố vào các kế hoạch về bảo đảm ATTT mạng, ứng dụng CNTT.

Điều 9. Trách nhiệm của các phòng, đơn vị thuộc xã

- Phối hợp với Văn phòng HĐND và UBND trong quá trình tham gia ứng cứu sự cố an toàn thông tin.

- Tổ chức tuyên truyền, phổ biến các văn bản quy phạm pháp luật nhằm nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin

- Tuân thủ phương án, kịch bản ứng cứu sự cố cho hệ thống thông tin; thông báo kịp thời các vấn đề bất thường liên quan tới an toàn thông tin cho Văn phòng HĐND và UBND.

Trong quá trình thực hiện Kịch bản này nếu có vấn đề vướng mắc, phát sinh, các phòng, đơn vị trực thuộc phản ánh kịp thời về Văn phòng HĐND và UBND để tổng hợp báo cáo./.