

Số: /QĐ-UBND

Phù Liễn, ngày tháng 8 năm 2025

QUYẾT ĐỊNH

**Về việc ban hành phương án, kịch bản ứng cứu sự cố
hệ thống thông tin phường Phù Liễn**

CHỦ TỊCH ỦY BAN NHÂN DÂN PHƯỜNG PHÙ LIỄN

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

*Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015; Luật An ninh mạng
ngày 12/06/2018;*

*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 Quyết định số 584/QĐ-UBND, ngày 28/02/2025 của UBND
thành phố Hải Phòng về việc điều chuyển chức năng, nhiệm vụ, bộ máy và biên
chế tại một số cơ quan chuyên môn thuộc UBND thành phố;*

*Căn cứ Công văn số 916/CAHP-ANM, ngày 14/4/2025 của Công an thành
phố Hải Phòng về việc thực hiện công tác bảo đảm an ninh mạng và an toàn thông tin;*

Theo đề nghị của Trưởng Công an phường Phù Liễn,

QUYẾT ĐỊNH:

Điều 1. Ban hành theo Quyết định này phương án, kịch bản ứng cứu sự cố
hệ thống thông tin phường Phù Liễn.

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

Điều 3. Chánh Văn phòng HĐND và UBND phường, Giám đốc Trung tâm
Phục vụ hành chính công, Trưởng công an phường; Thủ trưởng các phòng, ban,
ngành và hiệu trưởng các cơ sở giáo dục trên địa bàn phường; các cơ quan, đơn
vị liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Công an thành phố;
- Sở Khoa học và Công nghệ;
- TT Đảng ủy, TT HĐND phường;
- Chủ tịch, các PCT UBND phường;
- Lưu: VT, CAP.

CHỦ TỊCH

Phạm Văn Diên

PHƯƠNG ÁN, KỊCH BẢN ỨNG CỨU SỰ CỐ MẠNG HỆ THỐNG THÔNG TIN

(Ban hành kèm theo Quyết định số /QĐ-UBND ngày tháng 8 năm 2025
của Ủy ban nhân dân phường Phù Liễn)

CHƯƠNG I CÁC QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

Các phòng, trung tâm, đơn vị, cán bộ công chức, viên chức, người lao động thuộc quản lý của Ủy ban nhân dân phường Phù Liễn.

Điều 2. Nguyên tắc, phương châm ứng phó 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 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.

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:

Công an phường Phù Liễn là bộ phận chuyên trách ứng cứu sự cố ATTT mạng của phường 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 phường.

Các phòng, trung tâm, 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).

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 tình 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 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.

* 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 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 phường, khi gặp sự cố trong quá trình sử dụng máy tính có kết nối mạng thực hiện thông báo ngay cho Công an phường.

Bước 2: Tiếp nhận sự cố

Công an phường tiếp nhận thông tin về sự cố qua các phương thức: điện thoại, trực tiếp, ...

Bước 3: Xác minh/xác nhận sự cố

Công an phường 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

Công an phường thực hiện phân loại sự cố (các loại sự cố ở Điều 5)

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

Ngay sau khi phân loại được sự cố Công an phường có trách nhiệm báo cáo Lãnh đạo đơn vị để xem xét loại sự cố và tùy theo đối tượng sẽ tiến hành xử lý.

Trường hợp sự cố được phân loại thông thường thì Công an phường 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 Công an thành phố) 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 Công an thành phố) 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.

Đội ứng cứu sự cố an toàn, an ninh mạng thành phố Hải Phòng được thành lập theo Quyết định số 3147/QĐ-UBND ngày 04/8/2025 của UBND thành phố.

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, 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 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 Công an phường

- 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 UBND phường.
- 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 Công an thành phố 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 hoạch về bảo đảm ATTT mạng, ứng dụng CNTT.

Điều 9. Trách nhiệm của các phòng, trung tâm, đơn vị thuộc phường

- Phối hợp với Công an phường 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 Công an phường.

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 Công an phường để tổng hợp báo cáo./.