ỦY BAN NHÂN DÂN THÀNH PHỐ HẢI PHÒNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 196 /KH-UBND	*Hải Phòng, ngày 20 tháng 8 năm 2018*

KẾ HOẠCH
Ứng phó sự cố an toàn thông tin mạng trên địa bàn thành phố Hải Phòng

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

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

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 Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020;

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

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 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 Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

Ủy ban nhân dân thành phố ban hành Kế hoạch ứng phó sự cố an toàn thông tin mạng trên địa bàn thành phố Hải Phòng như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin mạng của thành phố, trong đó tập trung an toàn thông tin cho các hệ thống thông tin quan trọng của thành phố, có khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin mạng. Đề ra các giải pháp ứng phó khi gặp sự cố mất an toàn thông tin mạng.

- Nâng cao năng lực, hiệu quả hoạt động mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia trên địa bàn thành phố, gắn kết với các đơn vị thành viên, hợp tác, kết nối chặt chẽ, điều phối kịp thời, phối hợp đồng bộ, hiệu quả của các lực lượng để ứng cứu sự cố mạng, chống tấn công mạng.

- Bảo đảm các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố bảo đảm an toàn thông tin mạng.

2. Yêu cầu

- Phải khảo sát, đánh giá các nguy cơ, sự cố an toàn thông tin mạng của hệ thống thông tin để đưa ra phương án đối phó, ứng cứu sự cố phù hợp, kịp thời.

- Phương án đối phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra được 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.

II. NHIỆM VỤ TRIỂN KHAI

1. Tuyên truyền, phổ biến các văn bản quy phạm pháp luật; tập huấn nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng

- Tổ chức hội nghị tuyên truyền, phổ biến về Luật An toàn thông tin mạng; 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; Quyết định số 898/QĐ-TTg ngày 27/5/2016 của Thủ tướng Chính phủ phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020; Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP; Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

- Tập huấn nâng cao nhận thức, kiến thức, kỹ năng về an toàn thông tin mạng cho cán bộ, công chức, viên chức.

- Đơn vị thực hiện: Sở Thông tin và Truyền thông; các sở, ban, ngành thành phố, Ủy ban nhân dân các quận, huyện và các đơn vị có liên quan.

- Thời gian thực hiện: hàng năm.

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

Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của các hệ thống thông tin và các đối tượng cần bảo vệ; 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; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố; 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*).

- Đơn vị thực hiện: Các sở, ban, ngành thành phố và Ủy ban nhân dân các quận, huyện.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông; Đội ứng cứu sự cố của thành phố; Nhà thầu cung cấp dịch vụ an toàn thông tin mạng *(nếu có)*; các đơn vị liên quan khác.

- Thời gian thực hiện: Thường xuyên trong năm hoặc đột xuất.

3. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi hệ thống thông tin cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Trong phương án đối phó, ứng cứu phải đặt ra được 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:

a) 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 của 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 v.v...

b) 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....

c) 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

▪ Ban Chỉ đạo Ứng dụng công nghệ thông tin thành phố có trách nhiệm:

- Chỉ đạo công tác điều phối, ứng cứu sự cố an toàn thông tin mạng trên địa bàn thành phố; chỉ đạo các cơ quan, đơn vị trực thuộc phối hợp, tuân thủ yêu cầu của Cơ quan điều phối quốc gia trong điều phối, ứng cứu sự cố.

- Triệu tập, chỉ đạo Đội ứng cứu sự cố của thành phố theo đề xuất của đơn vị chuyên trách ứng cứu sự cố.

▪ Chủ quản hệ thống thông tin chỉ đạo các đơn vị chuyên môn tham mưu, phối hợp với các tổ chức tư vấn, cung cấp dịch vụ (nếu có) để triển khai các biện pháp bảo đảm an toàn thông tin cho các hệ thống thông tin như sau:

- Chủ động thực hiện giám sát theo quy định hiện hành.

- Khảo sát, kiểm tra, đánh giá an toàn thông tin cho các hệ thống thông tin quan trọng hoặc có nguy cơ bị tấn công cao.

- Xây dựng và triển khai các phương án khắc phục điểm yếu (nếu có), bảo vệ hoặc phòng ngừa để giảm thiểu thiệt hại khi có tấn công, sự cố an toàn thông tin mạng.

- Triển khai các biện pháp sao lưu dự phòng để nâng cao khả năng phục hồi hệ thống khi xảy ra sự cố.

▪ Các đơn vị được giao quản lý, vận hành hệ thống thông tin:

- Tăng cường theo dõi, giám sát các hoạt động của hệ thống thông tin để phát hiện ra các vấn đề bất thường, dấu hiệu tấn công, sự cố an toàn thông tin mạng. Khi phát hiện sự cố an toàn thông tin, thực hiện xử lý theo quy trình được hướng dẫn tại Điều 10, 11 Thông tư số 20/2017/TT-BTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông.

- Chấp hành quy định về thông báo, báo cáo sự cố an toàn thông tin mạng tại Điều 9 Thông tư số 20/2017/TT-BTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông.

▪ Sở Thông tin và Truyền thông có trách nhiệm:

- Thông báo ngay thông tin sự cố đến đơn vị vận hành hệ thống thông tin, cơ quan chủ quản hệ thống thông tin và các cơ quan chức năng liên quan.

- Phản hồi cho tổ chức, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố.

- Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo Ban Chỉ đạo Ứng dụng công nghệ thông tin thành phố và Cơ quan điều phối quốc gia; đề xuất, xin ý kiến chỉ đạo trong trường hợp không thuộc thẩm quyền, phạm vi trách nhiệm của mình hoặc vượt khả năng xử lý của mình.

▪ Đội ứng cứu sự cố an toàn thông tin mạng thành phố:

- Phối hợp với Cơ quan điều phối quốc gia về ứng cứu sự cố, các thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia, bộ phận tác nghiệp ứng cứu khẩn cấp quốc gia, các Đội ứng cứu của các tỉnh, thành phố khác để triển khai hoạt động ứng cứu sự cố an toàn thông tin mạng khi có yêu cầu.

- Phối hợp, hỗ trợ Văn phòng Thành ủy, Văn phòng Ủy ban nhân dân thành phố, Văn phòng Hội đồng nhân dân thành phố, các sở, ban, ngành thành phố, Ủy ban nhân dân các quận, huyện về công tác ứng cứu các sự cố an toàn thông tin mạng theo thẩm quyền, trách nhiệm và khả năng xử lý của Đội ứng cứu.

đ) Phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ và dự kiến kinh phí để thực hiện, đối phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể

- Đơn vị chủ trì: Các sở, ban, ngành thành phố và Ủy ban nhân dân cấp huyện.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông; Đội ứng cứu sự cố an toàn thông tin mạng của thành phố; Nhà thầu cung cấp dịch vụ an toàn thông tin mạng (*nếu có*); các đơn vị khác có liên quan.

- Thời gian thực hiện: Hàng năm.

4. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố

Triển khai các hoạt động thuộc trách nhiệm của các cơ quan, đơn vị liên quan theo quy định tại các Điều 11, Điều 12, Điều 13, Điều 14 và các nội dung liên quan khác của Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (*sau đây gọi tắt là Quyết định số 05/2017/QĐ-TTg*).

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 khi có sự cố xảy ra.

4.1. Báo cáo sự cố an toàn thông tin mạng theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg và Điều 9 Thông tư số 20/2017/TT-BTTTT

- Đơn vị thực hiện: Đơn vị quản lý, vận hành hệ thống thông tin, Chủ quản hệ thống thông tin.

- Đơn vị phối hợp: Sở Thông tin và Truyền thông, Đội ứng cứu sự cố an toàn thông tin mạng của thành phố.

- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

4.2. Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg và Điều 10 Thông tư số 20/2017/TT-BTTTT

- Đơn vị chủ trì: Đơn vị quản lý, vận hành hệ thống thông tin (*các sở, ban, ngành; Ủy ban nhân dân cấp huyện*); Đội ứng cứu sự cố của thành phố; Sở Thông tin và Truyền thông.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia về ứng cứu sự cố, Ban Chỉ đạo Ứng dụng công nghệ thông tin thành phố; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; đơn vị cung cấp dịch vụ an toàn thông tin mạng (*nếu có*); các đơn vị chức năng liên quan.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố của tổ chức, cá nhân.

4.3. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg và Điều 11 Thông tư số 20/2017/TT-BTTTT

5. Triển khai huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố, cụ thể bao gồm:

5.1. Triển khai các chương trình huấn luyện, diễn tập

Huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; huấn luyện, diễn tập nâng cao kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố; tham gia huấn luyện, diễn tập vùng, miền, quốc gia, quốc tế.

- Đơn vị chủ trì: Sở Thông tin và Truyền thông; Đội ứng cứu sự cố của thành phố.

- Đơn vị phối hợp: Đơn vị quản lý, vận hành hệ thống thông tin; các sở, ban, ngành, Ủy ban nhân dân các quận, huyện; Cơ quan điều phối quốc gia về ứng cứu sự cố an toàn thông tin mạng; các đơn vị chức năng liên quan.

- Thời gian thực hiện: Hàng năm.

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

Giám sát, phát hiện sớm nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin 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.

- Đơn vị chủ trì: các sở, ban, ngành thành phố, Ủy ban nhân dân các quận, huyện.

- Đơn vị phối hợp: Đội ứng cứu sự cố của thành phố; Sở Thông tin và Truyền thông; Cơ quan điều phối quốc gia về ứng cứu sự cố; các đơn vị chức năng liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

5.3. 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.

- Đơn vị chủ trì: các sở, ban, ngành thành phố, Ủy ban nhân dân các quận, huyện.

- Thời gian thực hiện: Hàng năm.

III. KINH PHÍ THỰC HIỆN

1. Nhu cầu kinh phí: dự toán Kế hoạch ngân sách hàng năm

2. Nguồn kinh phí: kinh phí sự nghiệp Công nghệ thông tin.

IV. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành, Ủy ban nhân dân các quận, huyện

- Xây dựng nội dung, lập dự toán kinh phí trong Kế hoạch ứng dụng công nghệ thông tin hàng năm của cơ quan, đơn vị để triển khai các nhiệm vụ được giao tại Kế hoạch này.

- Phân công lãnh đạo phụ trách và thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về an toàn thông tin mạng của cơ quan, đơn vị.

- Thực hiện xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 và Điều 15 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 và theo hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Sở Thông tin và Truyền thông

- Là cơ quan thường trực triển khai thực hiện Kế hoạch này.

- Thẩm định, phê duyệt hoặc cho ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo thẩm quyền quy định tại Khoản 1, Khoản 2 Điều 12 và Khoản 5 Điều 15 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 và theo hướng dẫn tại Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Theo dõi, đôn đốc, kiểm tra, giám sát công tác bảo đảm an toàn thông tin đối với các sở, ban, ngành, Ủy ban nhân dân các quận, huyện trên địa bàn thành phố.

- Xây dựng nội dung, lập dự toán kinh phí trong Kế hoạch ứng dụng công nghệ thông tin hằng năm của thành phố để thực hiện các nhiệm vụ được giao tại Kế hoạch này.

3. Sở Kế hoạch và Đầu tư, Sở Tài chính

Căn cứ các nhiệm vụ trong Kế hoạch để thẩm định, tham mưu bố trí ngân sách nhà nước hàng năm của thành phố cho các cơ quan, đơn vị triển khai Kế hoạch này.

Ủy ban nhân dân thành phố yêu cầu Thủ trưởng các sở, ban, ngành thành phố; Chủ tịch Ủy ban nhân dân các quận, huyện nghiêm túc triển khai thực hiện. Trong quá trình thực hiện nếu có vướng mắc, khó khăn, các đơn vị, địa phương phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân thành phố./.

Nơi nhận:
- Bộ Thông tin và Truyền thông;
- TTTU, TT HĐND TP;
- CT, các PCT UBND TP;
- Ủy ban MTTQVN TP;
- Văn phòng: Thành ủy, Đoàn ĐBQH, HĐND TP;
- Các sở, ban, ngành TP;
- UBND các quận, huyện;
- CVP, các PCVP;
- Phòng KTGSTĐKT;
- CV: GD;
- Lưu: VT.

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

Nguyễn Xuân Bình