UỶ BAN NHÂN DÂN **TỈNH HẢI DƯƠNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2308/KH-UBND	*Hải Dương, ngày 08 tháng 8 năm 2017*

KẾ HOẠCH
Ứng phó sự cố đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Hải Dương

Căn cứ Luật Công nghệ thông tin số 67/2006/QH11 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 về 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 24/04/2017 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;

Xét đề nghị của Sở Thông tin và Truyền thông tại Tờ trình số 688/TTr-STTTT ngày 20/7/2017;

Ủy ban nhân dân tỉnh ban hành Kế hoạch ứng phó sự cố đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Hải Dương, như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

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

b) Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với lực lượng cán bộ, công chức, viên chức.

c) Đảm bảo 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

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

b) 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.

- 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 chủ trì: Sở Thông tin và Truyền thông.

- Đơn vị phối hợp: Các Sở, ngành; UBND cấp huyện; các đơn vị có liên quan của tỉnh.

- Thời gian thực hiện: Trong năm 2017 và các năm tiếp theo.

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, ngành ; UBND cấp huyện của tỉnh.

- Đơn vị phối hợp: Đơn vị chuyên trách ứng cứu sự cố (*Sở Thông tin và Truyền thông*); Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh; 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.

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

Đối với mỗi hệ thống thông tin, chương trình, ứng dụng, 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;

d) 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, ngành; UBND cấp huyện của tỉnh.

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

- 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.

a) Báo cáo sự cố an toàn thông tin mạng theo quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg

- Đơn vị thực hiện:

+ Đơn vị vận hành hệ thống thông tin (*các Sở, ngành; UBND cấp huyện*) báo cáo Chủ quản hệ thống thông tin, Sở Thông tin và Truyền thông, đồng gửi Cơ quan điều phối quốc gia (*Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam – VNCERT, địa chỉ: 115 Trần Duy Hưng, Trung Hòa, Cầu Giấy, Hà Nội, Website: www.vncert.gov.vn*);

+ Sở Thông tin và Truyền thông báo cáo Chủ quản hệ thống thông tin, Ban chỉ đạo CNTT tỉnh và Cơ quan điều phối quốc gia;

+ Ban Chỉ đạo ứng cứu sự cố của tỉnh báo cáo Cơ quan thường trực và Ban Chỉ đạo quốc gia về ứng cứu sự cố.

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

b) 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

- Đơn vị chủ trì: Sở Thông tin và Truyền thông; Đơn vị vận hành hệ thống thông tin (*các Sở, ngành; UBND cấp huyện*); Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh.

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (*Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam – VNCERT*); Ban chỉ đạo CNTT tỉnh; 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.

c) 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

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:

a) 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 bảo đảm an toàn thông tin mạng của tỉnh.

- **Đơn vị phối hợp:** Đơn vị vận hành hệ thống thông tin (*các Sở, ngành; UBND cấp huyện*); Cơ quan điều phối quốc gia (*Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam – VNCERT*); các đơn vị chức năng liên quan.

- **Thời gian thực hiện:** Hàng năm.

b) 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:** Sở Thông tin và Truyền thông; Đơn vị vận hành hệ thống thông tin (*các Sở, ngành; UBND cấp huyện*); Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh.

- **Đơn vị phối hợp:** Cơ quan điều phối quốc gia (*Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam – VNCERT*); các đơn vị chức năng liên quan.

- **Thời gian thực hiện:** Thường xuyên trong năm.

c) 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; chuẩn bị các điều kiện bảo đảm, dự phòng các nguồn lực và tài chính để sẵn sàng đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của đội ứng cứu sự cố; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- **Đơn vị chủ trì:** Sở Thông tin và Truyền thông; Đơn vị vận hành hệ thống thông tin (*các Sở, ngành; UBND cấp huyện*); Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh.

- **Đơn vị phối hợp:** Cơ quan điều phối quốc gia (*Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam – VNCERT*); các đơn vị chức năng liên quan.

- **Thời gian thực hiện:** Hàng năm.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện được sử dụng từ nguồn ngân sách tỉnh.

IV. TỔ CHỨC THỰC HIỆN

1. Các Sở, ngành; UBND cấp huyện

- Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch ứng dụng công nghệ thông tin hàng năm của cơ quan, đơn vị mình 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 24/04/2017 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.

- Định kỳ hằng năm, gửi báo cáo tình hình, kết quả về Sở Thông tin và Truyền thông để tổng hợp báo cáo UBND tỉnh hoặc báo cáo đột xuất khi cấp trên có yêu cầu.

2. Sở Thông tin và Truyền thông

- Tham mưu, trình UBND tỉnh quyết định thành lập Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh.

- Là thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia; làm đầu mối, tổ chức hoạt động ứng cứu sự cố, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn thông tin mạng trên địa bàn tỉnh; tham gia hoạt động ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia khi có yêu cầu từ Cơ quan thường trực hoặc Cơ quan điều phối.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát công tác bảo đảm an toàn thông tin định kỳ hằng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh.

- 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 24/04/2017 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, hướng dẫn, kiểm tra, giám sát việc thực hiện ứng phó sự cố đảm bảo an toàn thông tin mạng ở các Sở, ban, ngành, UBND cấp huyện.

- Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch ứng dụng công nghệ thông tin hằng năm của tỉnh để đảm bảo cho hoạt động của Ban Ban chỉ đạo CNTT tỉnh, Đơn vị chuyên trách ứng cứu sự cố (*Sở Thông tin và Truyền thông*), Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh, gồm: Kinh phí để triển khai các hoạt động liên quan thuộc trách nhiệm của tỉnh quy định tại các Điều 7, Điều 11, Điều 12, Điều 13, Điều 14 và Điều 16 Quyết

định số 05/2017/QĐ-TTg; kinh phí triển khai Kế hoạch ứng phó sự cố của tỉnh; kinh phí dự phòng ứng cứu, xử lý sự cố cho các hệ thống thông tin thuộc tỉnh quản lý; kinh phí tổ chức đào tạo, huấn luyện, diễn tập và hoạt động của Đội ứng cứu sự cố bảo đảm an toàn thông tin mạng của tỉnh; kinh phí giám sát, kiểm tra, rà quét, đánh giá an toàn thông tin; hỗ trợ xây dựng, áp dụng chuẩn ISO 27xxx và triển khai các hoạt động nghiệp vụ đặc thù bảo đảm an toàn thông tin mạng cho các hệ thống thông tin thuộc tỉnh quản lý.

- Lập Báo cáo sơ kết 6 tháng triển khai Quyết định số 05/2017/QĐ-TTg (*trước ngày 20/6*) và Báo cáo tổng kết hàng năm thực hiện Quyết định số 05/2017/QĐ-TTg (*trước ngày 20/12*), gửi Bộ Thông tin và Truyền thông. Đồng thời, thực hiện báo cáo đột xuất khi khi cấp trên có yêu cầu.

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 hằng năm của tỉnh, cho các cơ quan, đơn vị, đảm bảo thực hiện triển khai tốt Kế hoạch.

Trên đây là Kế hoạch Ứng phó sự cố đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Hải Dương, yêu cầu Thủ trưởng các Sở, ban, ngành thuộc UBND tỉnh; Chủ tịch UBND cấp 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, kiến nghị về Sở Thông tin và Truyền thông để tổng hợp báo cáo Chủ tịch UBND tỉnh./.

CHỦ TỊCH

Nguyễn Dương Thái

Nơi nhận:
- Bộ Thông tin và Truyền thông; (*Để báo cáo*)
- Bộ Nội vụ;
- Thường trực Tỉnh ủy;
- Chủ tịch, các PCT UBND tỉnh;
- Lãnh đạo VP UBND tỉnh;
- Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (*115 Trần Duy Hưng, Trung Hòa, Cầu Giấy, Hà Nội*);
- Các Sở, ngành trực thuộc UBND tỉnh;
- Ban Quản lý các KCN tỉnh;
- UBND các huyện, thị xã, thành phố;
- Trung tâm CNTT – VP UBND tỉnh;
- Lưu: VT. (46)Nam