BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 20 /2017/TT-BTTTT	

Hà Nội, ngày 12 tháng 9 năm 2017

THÔNG TƯ

Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc

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

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 Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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;

Theo đề nghị của Giám đốc Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam;

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Thông tư này quy định về các hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc (không bao gồm hoạt động điều phối ứng cứu sự cố an toàn thông tin mạng nghiêm trọng quy định tại Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 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 (sau đây gọi tắt là Quyết định số 05/2017/QĐ-TTg));

Các sự cố của hệ thống thông tin do Bộ Quốc phòng, Bộ Công an quản lý không thuộc phạm vi điều chỉnh của Thông tư này.

2. Đối tượng áp dụng là các cơ quan, tổ chức, cá nhân có liên quan tới hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng.

Điều 2. Giải thích từ ngữ

1. *Sự cố an toàn thông tin mạng* là việc thông tin, hệ thống thông tin bị tấn công hoặc gây nguy hại, ảnh hưởng tới tính nguyên vẹn, tính bảo mật hoặc tính

khả dụng (sau đây gọi tắt là sự cố).

2. *Ứng cứu sự cố an toàn thông tin mạng* là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng gồm: theo dõi, thu thập, phân tích, phát hiện, cảnh báo, điều tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

3. *Đầu mối ứng cứu sự cố* là bộ phận hoặc cá nhân được thành viên mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia cử để thay mặt cho thành viên liên lạc và trao đổi thông tin với Cơ quan điều phối quốc gia về ứng cứu sự cố hoặc các thành viên khác trong hoạt động điều phối, ứng cứu sự cố.

Điều 3. Phân cấp tổ chức thực hiện ứng cứu sự cố bảo đảm an toàn thông tin mạng trên toàn quốc

Phân cấp tổ chức thực hiện ứng cứu sự cố bảo đảm an toàn thông tin mạng trên toàn quốc là các cơ quan, tổ chức, đơn vị thực hiện ứng cứu sự cố bảo đảm an toàn thông tin mạng quốc gia được quy định tại Quyết định số 05/2017/QĐ-TTg. Các cơ quan, tổ chức tham gia hoạt động điều phối, ứng cứu sự cố trên toàn quốc gồm:

1. Bộ Thông tin và Truyền thông - Cơ quan thường trực về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (gọi tắt là Cơ quan thường trực quốc gia) và Ban điều phối ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (gọi tắt là Ban điều phối ứng cứu quốc gia); Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam VNCERT - Cơ quan điều phối quốc gia về ứng cứu sự cố (gọi tắt là Cơ quan điều phối quốc gia).

2. Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng của các Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương (gọi tắt là Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh).

3. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng (sau đây gọi tắt là Đơn vị chuyên trách về ứng cứu sự cố); Đội ứng cứu sự cố hoặc bộ phận ứng cứu sự cố tại Bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và Ủy ban nhân dân các tỉnh, thành phố trực thuộc Trung ương (sau đây gọi tắt là Đội/bộ phận ứng cứu sự cố).

4. Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia (gọi tắt là Mạng lưới ứng cứu sự cố); và Ban Điều hành mạng lưới.

5. Chủ quản hệ thống thông tin; đơn vị vận hành hệ thống thông tin; các cơ quan, tổ chức, đơn vị chuyên môn được Cơ quan thường trực, Cơ quan điều phối quốc gia hoặc Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh chỉ định hoặc triệu tập tham gia ứng cứu sự cố.

Điều 4. Nguyên tắc điều phối, ứng cứu 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 cơ quan, tổ chức, doanh nghiệp trong nước và nước ngoài.

4. Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

5. Tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động của hệ thống thông tin đã được cấp thẩm quyền phê duyệt trong kế hoạch ứng phó sự cố.

6. Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

7. Bảo đảm bí mật thông tin biết được khi tham gia, thực hiện các hoạt động ứng cứu sự cố theo yêu cầu của Cơ quan điều phối quốc gia hoặc cơ quan, tổ chức, cá nhân gặp sự cố.

Chương II

MẠNG LƯỚI ỨNG CỨU SỰ CỐ

Điều 5. Mạng lưới ứng cứu sự cố

1. Mạng lưới ứng cứu sự cố hoạt động trên toàn quốc, gồm thành viên là các đơn vị chuyên trách về ứng cứu sự cố và các cơ quan, tổ chức, doanh nghiệp liên quan được quy định chi tiết tại Điều 7 Quyết định số 05/2017/QĐ-TTg.

2. Mạng lưới ứng cứu sự cố hoạt động theo Quy chế hoạt động của Mạng lưới và hướng dẫn liên quan của Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam). Ban điều hành mạng lưới do Bộ Thông tin và Truyền thông thành lập theo quy định tại Điều 7 Quyết định số 05/2017/QĐ-TTg.

3. Các thành viên mạng lưới khai báo hồ sơ theo Biểu mẫu số 01 ban hành kèm theo Thông tư này, định kỳ cập nhật hàng năm, gửi Cơ quan điều phối quốc gia. Các tổ chức, doanh nghiệp, cá nhân tự nguyện đăng ký tham gia mạng lưới phải có đơn đăng ký tham gia theo Biểu mẫu số 02, gửi Cơ quan điều phối quốc gia.

Điều 6. Trách nhiệm, quyền hạn của các thành viên mạng lưới

1. Thành viên mạng lưới có các trách nhiệm và quyền hạn sau:

a) Thực hiện các trách nhiệm và quyền hạn quy định tại Quyết định số 05/2017/QĐ-TTg;

b) Cử Đầu mối ứng cứu sự cố có đủ năng lực, trình độ chuyên môn và kỹ năng nghiệp vụ để thực hiện các hoạt động phối hợp ứng cứu sự cố; bảo đảm duy trì liên lạc thông suốt, liên tục 24/7; công bố thông tin về địa chỉ tiếp nhận sự cố trên Trang/Cổng thông tin điện tử; cung cấp, cập nhật thông tin về Đầu mối ứng cứu sự cố, nhân lực kỹ thuật an toàn thông tin, ứng cứu sự cố thuộc phạm vi quản lý tới Cơ quan điều phối quốc gia; cập nhật thông tin về Đầu mối

ứng cứu sự cố, trong vòng 24 giờ khi có thay đổi;

c) Tổng hợp, xây dựng báo cáo định kỳ 06 tháng (trước ngày 20 tháng 6), 01 năm (trước ngày 15 tháng 12) theo Biểu mẫu số 05 gửi Cơ quan điều phối quốc gia; báo cáo đột xuất khi có yêu cầu của Cơ quan điều phối quốc gia;

d) Báo cáo với Cơ quan điều phối quốc gia khi tiếp nhận thông tin, phát hiện các sự cố đối với hệ thống thông tin trong phạm vi quản lý;

đ) Xây dựng và triển khai kế hoạch ứng phó sự cố, hướng dẫn hoạt động ứng cứu sự cố, tổ chức và điều hành hoạt động của Đội ứng cứu sự cố trong phạm vi quản lý;

e) Có quyền đề nghị thành viên mạng lưới hướng dẫn, hỗ trợ xử lý và ứng cứu sự cố khi cần thiết; được tham gia các hội thảo, hội nghị giao ban, tập huấn, bồi dưỡng, đào tạo, huấn luyện, diễn tập và các hoạt động khác trong mạng lưới;

g) Có quyền được chia sẻ thông tin, kinh nghiệm, cảnh báo về sự cố và tình hình an toàn thông tin mạng trong và ngoài nước;

h) Các thành viên mạng lưới là cơ quan, đơn vị chức năng thuộc Bộ Công an và Bộ Quốc phòng không phải thực hiện Điểm c và Điểm d Khoản này.

2. Trách nhiệm và quyền hạn của Cơ quan điều phối quốc gia:

a) Thực hiện các trách nhiệm và quyền hạn quy định tại Quyết định số 05/2017/QĐ-TTg;

b) Công khai trên Trang thông tin điện tử của mình số điện thoại, số fax, địa chỉ thư điện tử (email), đường dây nóng và bảo đảm nguồn lực để duy trì trực đường dây nóng liên tục, kịp thời tiếp nhận và xử lý sự cố; tổng hợp thông tin liên lạc (địa chỉ, số điện thoại, số fax, địa chỉ thư điện tử) và thông tin về đầu mối ứng cứu sự cố, nhân lực kỹ thuật an toàn thông tin, ứng cứu sự cố của các thành viên mạng lưới và Đội ứng cứu sự cố của các thành viên mạng lưới;

c) Xây dựng, triển khai và vận hành cổng thông tin mạng lưới, hệ thống kỹ thuật hỗ trợ cho hoạt động liên lạc, trao đổi thông tin trong mạng lưới và các hệ thống kỹ thuật phục vụ các hoạt động điều phối, ứng cứu, xử lý, khắc phục sự cố;

d) Hướng dẫn hoạt động thông báo và hỏi đáp về sự cố an toàn thông tin mạng trên toàn quốc; điều hành mạng lưới; nghiên cứu, đề xuất các biện pháp nhằm tăng cường nguồn lực cho mạng lưới hoạt động có hiệu quả;

đ) Tập hợp, tiếp nhận, xử lý, chuẩn bị thông tin, cảnh báo tới người có thẩm quyền và các cơ quan, tổ chức, đơn vị liên quan về các nguy cơ, sự cố an toàn thông tin mạng và các biện pháp phòng ngừa, ngăn chặn, xử lý;

e) Tổ chức hội thảo, hội nghị giao ban, phổ biến, trao đổi thông tin, tập huấn, bồi dưỡng, đào tạo, huấn luyện, diễn tập về an toàn thông tin mạng, ứng cứu sự cố; tổ chức các hoạt động chung của mạng lưới.

Điều 7. Các hoạt động chính của mạng lưới ứng cứu sự cố

Ban điều hành mạng lưới tổ chức triển khai các nhiệm vụ của mạng lưới ứng cứu sự cố, gồm các hoạt động chính sau:

1. Nghiên cứu, thu thập, tiếp nhận, phân tích, xác minh, đánh giá, cảnh báo về sự cố, rủi ro an toàn thông tin mạng và phần mềm độc hại.

2. Phối hợp thực hiện ứng cứu, xử lý, ngăn chặn và khắc phục sự cố; kiểm tra, đốc thúc việc xây dựng, triển khai kế hoạch ứng phó sự cố an toàn thông tin mạng và việc thực hiện các trách nhiệm, nghĩa vụ của thành viên mạng lưới;

3. Xây dựng, nâng cao năng lực cho các thành viên mạng lưới và các Đội ứng cứu sự cố, gồm:

a) Huấn luyện, diễn tập, đào tạo, tập huấn nâng cao trình độ, kỹ năng và nghiệp vụ; tổ chức các chuyến công tác trong và ngoài nước để khảo sát, học hỏi kinh nghiệm, trao đổi, hợp tác;

b) Giao ban định kỳ, tổ chức hội thảo, hội nghị, tọa đàm trao đổi và chia sẻ thông tin, kinh nghiệm về điều phối, ứng cứu sự cố, bảo đảm an toàn thông tin mạng;

c) Hỗ trợ xây dựng và áp dụng các quy trình quản lý, vận hành hệ thống thông tin theo các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia và tiêu chuẩn quốc tế về an toàn thông tin, ứng cứu sự cố;

d) Tổ chức các nghiên cứu chuyên môn, xây dựng các báo cáo, tài liệu, hướng dẫn, thống kê về an toàn thông tin mạng và các vấn đề liên quan để chia sẻ, phổ biến trong mạng lưới.

4. Tham gia các hoạt động thông tin, tuyên truyền nâng cao nhận thức về phòng ngừa, ứng cứu sự cố, bảo đảm an toàn thông tin mạng.

5. Tổ chức, duy trì hoạt động của Ban điều hành mạng lưới; và triển khai các hoạt động khác liên quan đến điều phối, ứng cứu sự cố, bảo đảm an toàn thông tin mạng.

Chương III
HOẠT ĐỘNG ĐIỀU PHỐI, ỨNG CỨU SỰ CỐ

Điều 8. Hoạt động điều phối ứng cứu sự cố

1. Điều phối ứng cứu sự cố là hoạt động của Cơ quan điều phối quốc gia và cơ quan có thẩm quyền nhằm huy động, điều hành, phối hợp thống nhất các nguồn lực gồm: nhân lực, vật lực (trang thiết bị), tài lực (tài chính, ngân sách) để phòng ngừa, theo dõi, thu thập, phát hiện, cảnh báo sự cố; tiếp nhận, phân tích, xác minh, phân loại sự cố; điều hành, phối hợp, tổ chức ứng cứu sự cố, sẵn sàng, ứng phó, khắc phục sự cố nhằm giảm thiểu các rủi ro, thiệt hại do sự cố gây ra.

2. Cơ quan điều phối quốc gia thực hiện chức năng cảnh báo, điều phối ứng cứu sự cố trên toàn quốc; có quyền huy động, điều phối các thành viên

mạng lưới ứng cứu sự cố và các tổ chức, đơn vị liên quan phối hợp ngăn chặn, xử lý, khắc phục sự cố trên toàn quốc; ban hành và chịu trách nhiệm về các lệnh/yêu cầu điều phối theo Biểu mẫu số 06 ban hành kèm theo Thông tư này;

3. Các tác nghiệp của hoạt động điều phối ứng cứu sự cố:

a) Theo dõi, phân tích, phát hiện, cảnh báo các nguy cơ, đe dọa, lỗ hổng, sự cố, tấn công mạng và các giải pháp phòng ngừa sự cố;

b) Xây dựng, đề xuất phương án, kế hoạch ứng phó với sự cố;

c) Tổ chức huấn luyện, diễn tập ứng cứu sự cố, bảo đảm an toàn thông tin mạng;

d) Điều hành, huy động các nguồn lực để ứng cứu sự cố theo thẩm quyền; cung cấp các hỗ trợ kỹ thuật và thực hiện các biện pháp để đối phó, phòng chống tấn công mạng;

đ) Điều tra, phân tích, xác định nguồn gốc, cách thức, phương pháp tấn công để đối phó, ngăn chặn, đồng thời cảnh báo và hướng dẫn để ngăn ngừa sự cố lây lan diện rộng; thu thập, xây dựng báo cáo tổng hợp sự cố;

e) Chia sẻ, trao đổi, cung cấp thông tin giữa các cơ quan, tổ chức có trách nhiệm liên quan về ứng cứu sự cố, hoạt động điều phối ứng cứu sự cố và quá trình xử lý sự cố;

g) Các hoạt động khác liên quan đến ứng cứu sự cố theo quyết định Bộ Thông tin và Truyền thông.

4. Hình thức trao đổi thông tin về điều phối ứng cứu sự cố được thực hiện bằng một hoặc nhiều hình thức như: Công văn, thư điện tử, điện thoại, fax, nhắn tin đa phương tiện hoặc hệ thống kỹ thuật truyền thông tiên tiến; và đảm bảo tuân thủ theo các quy định pháp luật liên quan khi trao đổi thông tin mật.

Điều 9. Thông báo, báo cáo sự cố an toàn thông tin mạng

1. Các hình thức thông báo, báo cáo sự cố

a) Hình thức thông báo sự cố: Bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện hoặc thông qua hệ thống kỹ thuật báo cáo sự cố an toàn thông tin mạng theo hướng dẫn của Cơ quan điều phối quốc gia;

b) Hình thức báo cáo sự cố: Bằng văn bản giấy hoặc văn bản điện tử (có ký tên và đóng dấu hoặc chữ ký số của người có thẩm quyền).

2. Báo cáo sự cố an toàn thông tin mạng

a) Đơn vị, cá nhân vận hành hệ thống thông tin có trách nhiệm chậm nhất 05 ngày kể từ khi phát hiện sự cố phải thông báo các thông tin của sự cố theo nội dung tại Điểm a Khoản 3 Điều này (Thông báo sự cố) tới đồng thời các cơ quan, đơn vị sau: Chủ quản hệ thống thông tin, Cơ quan điều phối quốc gia, Đơn vị chuyên trách về ứng cứu sự cố và thành viên mạng lưới ứng cứu sự cố có trách nhiệm liên quan (nếu có). Tại thời điểm báo cáo, nếu chưa hoàn thành việc

xử lý sự cố, đơn vị, cá nhân vận hành hệ thống phải cập nhật lại thông tin của sự cố cho các cơ quan, đơn vị đã nhận thông tin trước đó ngay khi kết thúc việc xử lý sự cố;

b) Trường hợp đơn vị, cá nhân vận hành hệ thống thông tin xác định sự cố có thể vượt khả năng xử lý của mình phải xây dựng ngay Báo cáo ban đầu sự cố, báo cáo Chủ quản hệ thống thông tin, Đơn vị chuyên trách về ứng cứu sự cố chịu trách nhiệm ứng cứu (nếu có) và Cơ quan điều phối quốc gia; sau khi kết thúc ứng cứu sự cố, chậm nhất trong vòng 05 ngày phải hoàn thiện Báo cáo kết thúc ứng phó sự cố để báo cáo Chủ quản hệ thống thông tin và Cơ quan điều phối quốc gia. Cơ quan điều phối quốc gia chỉ ghi nhận sự cố đã hoàn thành ứng cứu sự cố sau khi đã nhận được Báo cáo kết thúc ứng phó sự cố;

c) Các tổ chức, cá nhân không phải là đơn vị, cá nhân vận hành hệ thống thông tin khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng thông báo thông tin của sự cố (Thông báo sự cố) tới đồng thời hoặc một trong các cơ quan, đơn vị sau: Đơn vị, cá nhân vận hành hệ thống thông tin, Chủ quản hệ thống thông tin, Cơ quan điều phối quốc gia, Đơn vị chuyên trách về ứng cứu sự cố hoặc thành viên mạng lưới ứng cứu sự cố có trách nhiệm liên quan.

3. Các loại thông báo, báo cáo sự cố:

a) Thông báo sự cố, nội dung gồm: Tên, địa chỉ đơn vị, cá nhân thông báo sự cố; tên hoặc tên miền, địa chỉ IP của hệ thống thông tin bị sự cố; tên, địa chỉ của đơn vị, cá nhân vận hành và cơ quan chủ quản hệ thống thông tin bị sự cố (nếu biết); mô tả sự cố và thời điểm phát hiện sự cố; kết quả xử lý sự cố, đề xuất, kiến nghị và các thông tin liên quan khác (nếu có);

b) Báo cáo ban đầu sự cố, nội dung theo Biểu mẫu số 03 Phụ lục I ban hành kèm theo Thông tư này;

c) Báo cáo diễn biến tình hình;

d) Báo cáo phương án ứng cứu cụ thể;

đ) Báo cáo đề nghị hỗ trợ, phối hợp;

e) Báo cáo kết thúc ứng phó sự cố, nội dung theo Biểu mẫu số 04 Phụ lục I ban hành kèm theo Thông tư này.

4. Trong quá trình ứng cứu sự cố, đơn vị, cá nhân vận hành hệ thống phải chủ trì, phối hợp với các cơ quan, đơn vị liên quan xây dựng và duy trì thực hiện các báo cáo ứng cứu sự cố theo quy định và yêu cầu của cơ quan có thẩm quyền.

Điều 10. Phát hiện, tiếp nhận, xác minh, xử lý ban đầu và phân loại sự cố an toàn thông tin mạng

1. Đơn vị, cá nhân vận hành hệ thống thông tin, có trách nhiệm:

a) Khi phát hiện sự cố: Tổ chức theo dõi, ghi chép và tập hợp các thông tin

liên quan đến sự cố và tổ chức thông báo hoặc báo cáo sự cố theo quy định tại Điều 9 của Thông tư này;

b) Khi tiếp nhận thông báo sự cố: Phản hồi ngay cho tổ chức, cá nhân gửi thông báo sự cố để xác nhận thông tin;

c) Xác minh sự cố và xử lý ban đầu: Chủ trì, phối hợp với đơn vị chịu trách nhiệm bảo đảm an toàn thông tin (nếu có), đơn vị chuyên trách về ứng cứu sự cố liên quan và các doanh nghiệp viễn thông, Internet (ISP) để tiến hành phân tích, xác minh, đánh giá sự cố; thực hiện ngay các hoạt động ứng cứu sự cố ban đầu, triển khai quy trình ứng cứu sự cố theo kế hoạch ứng phó sự cố an toàn thông tin mạng đã được cấp thẩm quyền phê duyệt hoặc quy trình tại Điều 11 của Thông tư này; trường hợp xác định sự cố có khả năng là sự cố nghiêm trọng, cần báo cáo ngay với chủ quản hệ thống thông tin, đơn vị chuyên trách về ứng cứu sự cố liên quan để đề xuất nâng cấp sự cố nghiêm trọng, đồng thời gửi Cơ quan điều phối quốc gia.

2. Đơn vị chuyên trách về ứng cứu sự cố hoặc thành viên mạng lưới ứng cứu sự cố, có trách nhiệm:

a) Khi phát hiện sự cố: Thông báo sự cố ngay đến đơn vị, cá nhân vận hành hệ thống thông tin, chủ quản hệ thống thông tin và Cơ quan điều phối quốc gia;

b) Khi tiếp nhận thông báo hoặc báo cáo sự cố: Ghi nhận, tiếp nhận đúng quy định và phản hồi cho tổ chức, cá nhân gửi thông báo hoặc báo cáo sự cố ngay sau khi nhận được để xác nhận thông tin;

c) Tổ chức xác minh và xử lý sự cố: Phối hợp với đơn vị, cá nhân vận hành hệ thống thông tin để thẩm tra, xác minh và xử lý sự cố trong khả năng và trách nhiệm của mình; trường hợp xác định sự cố có khả năng vượt qua khả năng xử lý của mình hoặc có khả năng là sự cố nghiêm trọng, cần báo cáo ngay chủ quản hệ thống thông tin và Cơ quan điều phối quốc gia;

d) Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo hoặc đề xuất, xin ý kiến chỉ đạo của chủ quản hệ thống thông tin và Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh trong trường hợp vượt thẩm quyền, phạm vi trách nhiệm của mình hoặc vượt khả năng xử lý của mình;

đ) Tổng hợp, báo cáo Cơ quan điều phối quốc gia về diễn biến sự cố khi được yêu cầu.

3. Cơ quan điều phối quốc gia có trách nhiệm:

a) Ghi nhận, tiếp nhận thông báo, báo cáo sự cố an toàn thông tin mạng theo đúng quy trình;

b) Phản hồi cho tổ chức, cá nhân gửi thông báo, báo cáo sự cố ngay sau khi nhận được để xác nhận thông tin;

c) Thẩm tra, xác minh và phân loại sự cố để thực hiện các cảnh báo, điều phối lựa chọn phương án, tổ chức ứng cứu và báo cáo, đề xuất với Cơ quan

thường trực xem xét, quyết định sự cố nghiêm trọng và phương án ứng cứu khẩn cấp phù hợp. Trường hợp phân loại là sự cố nghiêm trọng, Cơ quan điều phối quốc gia chủ trì, phối hợp với các cơ quan liên quan triển khai các bước theo quy trình ứng cứu sự cố nghiêm trọng quy định tại Quyết định số 05/2017/QĐ-TTg;

d) Tổ chức hoạt động phối hợp với các tổ chức ứng cứu sự cố mạng quốc tế để tiếp nhận các cảnh báo sớm, thông tin về sự cố, nguy cơ về mất an toàn thông tin mạng và phối hợp ứng cứu sự cố, tấn công xuyên biên giới;

đ) Thực hiện các trách nhiệm khác của Cơ quan điều phối quốc gia; báo cáo, đề xuất với Cơ quan thường trực các vấn đề vượt thẩm quyền.

Điều 11. Quy trình ứng cứu sự cố an toàn thông tin mạng

Quy trình ứng cứu sự cố an toàn thông tin mạng theo sơ đồ tại Phụ lục II, cụ thể gồm:

1. Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố

a) Tiếp nhận, xác minh sự cố

Đơn vị chủ trì: Đơn vị, cá nhân vận hành hệ thống thông tin.

Đơn vị phối hợp: Đơn vị chuyên trách về ứng cứu sự cố, Cơ quan điều phối quốc gia.

Nội dung thực hiện: Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài. Khi phân tích, xác minh sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố.

b) Triển khai các bước ưu tiên ứng cứu ban đầu

Đơn vị chủ trì: Đơn vị, cá nhân vận hành hệ thống thông tin.

Đơn vị phối hợp: Đơn vị chuyên trách về ứng cứu sự cố, thành viên mạng lưới có liên quan và Cơ quan điều phối quốc gia.

Nội dung: Sau khi đã xác định sự cố xảy ra, đơn vị, cá nhân vận hành hệ thống thông tin căn cứ vào bản chất, dấu hiệu của sự cố tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo kế hoạch ứng phó sự cố đã được cấp thẩm quyền phê duyệt hoặc theo hướng dẫn của Đơn vị chuyên trách về ứng cứu sự cố liên quan hoặc Cơ quan điều phối quốc gia.

c) Triển khai lựa chọn phương án ứng cứu

Đơn vị chủ trì: Đơn vị, cá nhân vận hành hệ thống thông tin.

Đơn vị phối hợp: Đơn vị chuyên trách về ứng cứu sự cố, thành viên mạng lưới có liên quan, Cơ quan điều phối quốc gia.

Nội dung thực hiện: Căn cứ theo kế hoạch ứng phó sự cố đã được cấp thẩm quyền phê duyệt hoặc theo hướng dẫn của Đơn vị chuyên trách về ứng cứu sự cố hoặc Cơ quan điều phối quốc gia để lựa chọn phương án ngăn chặn và xử lý sự cố; báo cáo, đề xuất Chủ quản hệ thống thông tin, Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh xin ý kiến chỉ đạo nếu cần.

d) Chỉ đạo xử lý sự cố (nếu cần)

Đơn vị chủ trì: Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh.

Đơn vị phối hợp: Chủ quản hệ thống thông tin.

Nội dung thực hiện: Căn cứ theo báo cáo, đề xuất của Đơn vị, cá nhân vận hành hệ thống thông tin, Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh phối hợp với chủ quản hệ thống thông tin và tham khảo ý kiến Cơ quan điều phối quốc gia (nếu cần) thực hiện chỉ đạo Đơn vị chuyên trách về ứng cứu sự cố, triệu tập Đội/bộ phận ứng cứu sự cố thuộc phạm vi quản lý triển khai công tác ứng cứu, xử lý sự cố; chỉ đạo, phân công hoạt động phát ngôn, cung cấp thông tin. Trong quá trình ứng cứu, tùy thuộc vào diễn biến tình hình thực tế, Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh có thể quyết định bổ sung thành phần tham gia Đội/bộ phận ứng cứu sự cố, chỉ đạo điều chỉnh phương án ứng cứu sự cố.

đ) Báo cáo sự cố

Đơn vị chủ trì: Đơn vị, cá nhân vận hành hệ thống thông tin.

Đơn vị phối hợp: Đơn vị chuyên trách về ứng cứu sự cố liên quan/chịu trách nhiệm, các doanh nghiệp viễn thông, Internet (ISP).

Nội dung thực hiện: Sau khi đã triển khai các bước ưu tiên ứng cứu ban đầu, Đơn vị vận hành hệ thống thông tin tổ chức thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan tổ chức theo quy định tại Điều 9 Thông tư này và quy định nội bộ (nếu có).

e) Điều phối công tác ứng cứu

Đơn vị chủ trì: Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh; Cơ quan điều phối quốc gia.

Đơn vị phối hợp: Đơn vị, cá nhân vận hành hệ thống thông tin, Đơn vị chuyên trách về ứng cứu sự cố, thành viên mạng lưới có liên quan.

Nội dung thực hiện: Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của Đơn vị, cá nhân vận hành hệ thống thông tin và Đơn vị chuyên trách về ứng cứu sự cố, Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh và Cơ quan điều phối quốc gia thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ứng cứu sự cố.

2. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

Đơn vị chủ trì: Đơn vị, cá nhân vận hành hệ thống thông tin; Đội/bộ phận ứng cứu sự cố.

Đơn vị phối hợp: Đơn vị chịu trách nhiệm bảo đảm an toàn thông tin cho hệ thống bị sự cố, Đơn vị chuyên trách về ứng cứu sự cố, thành viên mạng lưới có liên quan, Cơ quan điều phối quốc gia.

Nội dung thực hiện:

a) Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị

ảnh hưởng.

b) Triển khai phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

3. Xử lý sự cố, gỡ bỏ và khôi phục

a) Xử lý sự cố, gỡ bỏ

Đơn vị chủ trì: Đơn vị, cá nhân vận hành hệ thống thông tin; Đội/bộ phận ứng cứu sự cố.

Đơn vị phối hợp: Đơn vị chịu trách nhiệm bảo đảm an toàn thông tin cho hệ thống bị sự cố; Đơn vị chuyên trách về ứng cứu sự cố, thành viên mạng lưới có liên quan, Cơ quan điều phối quốc gia.

Nội dung thực hiện: Sau khi đã triển khai ngăn chặn sự cố, đơn vị, cá nhân vận hành hệ thống thông tin, Đơn vị chuyên trách về ứng cứu sự cố, Đội/bộ phận ứng cứu sự cố triển khai tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin.

b) Khôi phục

Đơn vị chủ trì: Đơn vị, cá nhân vận hành hệ thống thông tin;.

Đơn vị phối hợp: Đội/bộ phận ứng cứu sự cố, Đơn vị chịu trách nhiệm bảo đảm an toàn thông tin cho hệ thống bị sự cố, Đơn vị chuyên trách về ứng cứu sự cố, thành viên mạng lưới có liên quan, Cơ quan điều phối quốc gia.

Nội dung thực hiện: Đơn vị, cá nhân vận hành hệ thống chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục hệ thống thông tin, dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin cho hệ thống thông tin.

c) Kiểm tra, đánh giá hệ thống thông tin

Đơn vị chủ trì: Đơn vị, cá nhân vận hành hệ thống thông tin.

Đơn vị phối hợp: Đơn vị chịu trách nhiệm bảo đảm an toàn thông tin cho hệ thống bị sự cố, Đơn vị chuyên trách về ứng cứu sự cố, chủ quản hệ thống thông tin, Cơ quan điều phối quốc gia.

Nội dung thực hiện: Đơn vị, cá nhân vận hành hệ thống và các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức các bước tương ứng tại Khoản 2 và Khoản 3 của Điều này để xử lý dứt điểm, khôi phục hoạt động bình thường của hệ thống thông tin.

4. Tổng kết, đánh giá

Đơn vị chủ trì: Đơn vị, cá nhân vận hành hệ thống thông tin.

Đơn vị phối hợp: Đơn vị chuyên trách về ứng cứu sự cố; Đội/bộ phận ứng cứu sự cố; Chủ quản hệ thống thông tin; Ban Chỉ đạo ứng cứu sự cố cấp bộ,

tỉnh; Cơ quan điều phối quốc gia.

Nội dung thực hiện: Đơn vị, cá nhân vận hành hệ thống bị sự cố phối hợp với Đơn vị chuyên trách về ứng cứu sự cố và Đội/bộ phận ứng cứu sự cố triển khai tổng hợp toàn bộ các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ứng cứu sự cố, báo cáo Chủ quản hệ thống thông tin, Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh và Cơ quan điều phối quốc gia; tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai.

Chương IV
BIỆN PHÁP BẢO ĐẢM THỰC HIỆN ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

Điều 12. Xây dựng và triển khai kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng

1. Các cơ quan, tổ chức và doanh nghiệp xây dựng và triển khai kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng của cơ quan, tổ chức và doanh nghiệp mình, trong đó:

a) Đối với các hệ thống thông tin đã được phê duyệt cấp độ 04, cấp độ 05 hoặc thuộc Danh mục hệ thống thông tin quan trọng quốc gia, theo Đề cương Kế hoạch ứng phó sự cố an toàn thông tin mạng quy định tại Điều 16 của Quyết định số 05/2017/QĐ-TTg .

b) Đối với các hệ thống thông tin không thuộc Điểm a Khoản 1 Điều này, theo Phụ lục III ban hành kèm theo Thông tư này .

2. Các chủ quản hệ thống thông tin và cơ quan, đơn vị có thẩm quyền phê duyệt Kế hoạch ứng phó sự cố cần xác định các điều kiện, nguyên tắc ưu tiên để duy trì hoạt động của hệ thống thông tin khi triển khai ứng cứu sự cố và coi nội dung này là một yêu cầu bắt buộc trong Kế hoạch ứng phó sự cố.

3. Cơ quan điều phối quốc gia hướng dẫn việc xây dựng, triển khai kế hoạch ứng phó sự cố, dự phòng ứng cứu, xử lý sự cố an toàn thông tin mạng; tổ chức hoạt động huấn luyện, diễn tập theo vùng, miền và quốc gia, quốc tế; xây dựng kế hoạch và tổ chức định kỳ kiểm tra, đánh giá về việc triển khai phương án ứng phó sự cố an toàn thông tin mạng của các bộ, ngành, địa phương và của các tổ chức, doanh nghiệp.

Điều 13. Kinh phí

Kinh phí triển khai các hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc thực hiện theo quy định tại Điều 17 Quyết định số 05/2017/QĐ-TTg và các văn bản hướng dẫn liên quan.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 14. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 11 năm 2017 và bãi bỏ Thông tư số 27/2011/TT-BTTTT ngày 04 tháng 10 năm 2011 của Bộ Thông tin và Truyền thông quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam .

2. Trong quá trình thực hiện, nếu có vướng mắc, phát sinh, tổ chức, cá nhân có liên quan kịp thời phản ánh về Bộ Thông tin và Truyền thông (qua Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam) để xem xét, bổ sung và sửa đổi./.

***Nơi nhận*:**
- Thủ tướng Chính phủ; các Phó Thủ tướng Chính phủ;
- Văn phòng Chính phủ;
- Văn phòng Trung ương và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Văn phòng Quốc hội;
- Văn phòng Chủ tịch nước;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Toà án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- UBND các tỉnh, thành phố trực thuộc TW;
- Cơ quan Trung ương của các đoàn thể;
- Ủy ban quốc gia về ứng dụng CNTT;
- Ban Chỉ đạo an toàn thông tin quốc gia;
- Các Đơn vị chuyên trách về CNTT, ATTT của Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc TW;
- Công báo, Cổng Thông tin điện tử Chính phủ;
- Cục Kiểm tra VBQPPL (Bộ Tư pháp);
- Bộ TTTT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ, Cổng Thông tin điện tử Bộ;
- Lưu: VT, VNCERT (200).

BỘ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Trương Minh Tuấn

Phụ lục I

DANH MỤC MẪU BIỂU QUY ĐỊNH HOẠT ĐỘNG ĐIỀU PHỐI, ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG TRÊN TOÀN QUỐC

(Ban hành kèm theo Thông tư số 20 /2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông)

TT	Mẫu số	Tên Mẫu biểu
1	Mẫu số 01	**Bản khai hồ sơ thành viên mạng lưới ứng cứu sự cố**
2	Mẫu số 02	**Đơn xin đăng ký tham gia mạng lưới ứng cứu sự cố** *(Áp dụng cho tổ chức, doanh nghiệp và cá nhân tự nguyện tham gia mạng lưới ứng cứu sự cố mạng)*
3	Mẫu số 03	**Báo cáo ban đầu sự cố an toàn thông tin mạng**
4	Mẫu số 04	**Báo cáo kết thúc ứng phó sự cố**
5	Mẫu số 05	**Báo cáo tổng hợp tình hình tiếp nhận và xử lý sự cố an toàn thông tin mạng**
6	Mẫu số 06	**Lệnh/yêu cầu điều phối**

Mẫu số 01
Ban hành kèm theo Thông tư số 20 /2017/TT-BTTTT ngày 12.../9./2017 của Bộ trưởng Bộ Thông tin và Truyền thông

TÊN TỔ CHỨC
.....

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

BẢN KHAI HỒ SƠ THÀNH VIÊN MẠNG LƯỚI ỨNG CỨU SỰ CỐ

1. Thông tin chung về tổ chức

- Tên tổ chức: .....
- Tên cơ quan chủ quản: .....
- Địa chỉ: .....
- Điện thoại: ..... Fax: .....
- Email: ..... Website: .....
- Lãnh đạo phụ trách an toàn thông tin: ..... Chức vụ: .....

2. Thông tin tiếp nhận thông báo sự cố

- Địa chỉ: .....
- Số điện thoại cố định: ..... Số điện thoại di động: .....
- Số Fax: ..... Email: .....

3. Đầu mối ứng cứu sự cố

3.1. Đầu mối ứng cứu sự cố chính

- Họ và tên: ..... Chức vụ: .....
- Địa chỉ liên hệ: .....
- Số điện thoại cố định: ..... Số điện thoại di động: .....
- Số Fax: ..... Email: .....

3.2. Đầu mối ứng cứu sự cố dự phòng

- Họ và tên: ..... Chức vụ: .....
- Địa chỉ liên hệ: .....
- Số điện thoại cố định: ..... Số di động: .....
- Số Fax: ..... Email: .....

4. Giới thiệu về hoạt động của tổ chức

(Cung cấp cho Cơ quan điều phối quốc gia các thông tin về năng lực ứng cứu sự cố của tổ chức như nhân sự, công nghệ, kinh nghiệm, đối tượng phục vụ,...)

.....

5. Tên các hệ thống thông tin thuộc phạm vi phụ trách hoặc cung cấp dịch vụ:

▪ Cấp 1:	▪ Cấp 2:	▪ Cấp 3:	▪ Cấp 4:	▪ Cấp 5:
1.	1.	1.	1.	1.
2.	2.	2.	2.	2.
....	....	....	....	....

6. Thông tin về Danh sách nhân lực, chuyên gia an toàn thông tin, công nghệ thông tin và tương đương

(Cung cấp thông tin về nhân lực an toàn thông tin, công nghệ thông tin thuộc đơn vị hoặc các đơn vị liên quan trong phạm vi mình phụ trách theo mẫu Tổng hợp kèm theo Biểu mẫu 01 này)

Chúng tôi cam kết thông tin khai báo trong hồ sơ là chính xác và tuân thủ trách nhiệm, quyền hạn của thành viên mạng lưới, các quy định về hoạt động điều phối ứng cứu sự cố theo quy định pháp luật và hướng dẫn của Cơ quan điều phối quốc gia ban hành.

....., ngày ..... tháng ..... năm .....

NGƯỜI ĐẠI DIỆN THEO PHÁT LUẬT
(Ký tên, đóng dấu hoặc sử dụng chữ ký số)

[mẫu] TỔNG HỢP DANH SÁCH NHÂN LỰC, CHUYÊN GIA VỀ CÔNG NGHỆ THÔNG TIN (CNTT), AN TOÀN THÔNG TIN (ATTT) HOẶC TƯƠNG ĐƯƠNG

(Kèm theo Mẫu số 01)

1. Số lượng nhân lực liên quan đến CNTT, ATTT hoặc tương đương

TT	Phân loại	Số lượng (người)
1.1	**Số lượng cán bộ phân theo lĩnh vực đào tạo**	
a)	Chuyên ngành về CNTT	
b)	Chuyên ngành về ATTT	
c)	Chuyên ngành tương đương	
1.2	**Số lượng cán bộ phân theo trình độ đào tạo**	
a)	Trên đại học	
b)	Đại học	
c)	Cao đẳng	
d)	Trung cấp	
1.3	**Số lượng cán bộ có chứng chỉ về CNTT, ATTT hoặc tương đương**	
a)	Số cán bộ có chứng chỉ quốc tế	
b)	Số cán bộ có chứng chỉ trong nước	

2. Số lượng nhân lực có kinh nghiệm, được đào tạo về ATTT

TT	phân loại	Số lượng (người)
2.1	**Nhóm chuyên gia quản lý ATTT**	
a)	Quản lý ATTT cấp cao	
b)	Hệ thống quản lý ATTT	
c)	Quản trị hệ thống thông tin (hệ điều hành, ứng dụng)	
d)	Quản trị an toàn mạng và hạ tầng mạng	
đ)	Xây dựng chính sách đảm bảo ATTT	
2.2	**Nhóm chuyên gia kỹ thuật phòng thủ, chống tấn công**	
a)	Kỹ thuật tấn công và chống tấn công mạng, chống khủng bố, chống chiến tranh mạng	
b)	Phân tích mã độc, phòng chống mã độc và phần mềm gián điệp	
c)	Ứng cứu xử lý sự cố ATTT	
d)	Kiểm tra, giám sát và phân tích hệ thống, dò quét lỗ hổng bảo mật	
đ)	Phân tích sự cố ATTT	
e)	Điều tra, thu thập thông tin sự cố và chứng cứ điện tử	
g)	Giám sát, lọc nội dung thông tin trên mạng	
h)	Theo dõi, kiểm soát luồng thông tin trên mạng	
2.3	**Nhóm chuyên gia kỹ thuật bảo vệ an toàn hệ thống và ứng dụng**	
a)	Mã hóa, thám mã, che dấu và bảo mật nội dung thông tin	
b)	Chữ ký số, nhận dạng, xác thực	
c)	Tích hợp hệ thống ATTT	
d)	Tư vấn, thiết kế, xây dựng hệ thống mạng an toàn	
đ)	Lập trình đảm bảo an toàn (ứng dụng Web, cổng thông tin điện tử)	
e)	Đảm bảo an toàn hệ thống viễn thông, mạng di động, mạng không dây	
g)	Đảm bảo an toàn giao dịch điện tử, thanh toán trực tuyến, thương mại điện tử	
h)	Đảm bảo an toàn cơ sở dữ liệu	
2.4	**Nhóm chuyên gia kỹ thuật kiểm tra, đánh giá ATTT**	
a)	Tư vấn hợp chuẩn ATTT	
b)	Phân tích, quản lý rủi ro, duy trì hoạt động hệ thống thông tin	
c)	Đánh giá an toàn hệ thống và sản phẩm công nghệ thông tin	
d)	Kiểm tra, đánh giá an toàn ứng dụng Web và cổng thông tin điện tử	

3. Danh sách nhân lực về ATTT, CNTT hoặc tương đương

TT	Họ và tên	Tên trường, cơ sở đào tạo	Chuyên ngành đào tạo, bồi dưỡng	Văn bằng, chứng chỉ, trình độ về ATTT, CNTT hoặc tương đương	Tháng/năm tốt nghiệp
1					
2					
...					

Ghi chú: Văn bằng: TSKH, TS, Ths, Cử nhân, Kỹ sư .....

Mẫu số 02
Ban hành kèm theo Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

ĐƠN XIN ĐĂNG KÝ THAM GIA MẠNG LƯỚI ỨNG CỨU SỰ CỐ

(Áp dụng cho tổ chức, doanh nghiệp và cá nhân tự nguyện tham gia mạng lưới ứng cứu sự cố mạng)

I. Thông tin chung về tổ chức

1. Tên tổ chức: .....
2. Địa chỉ: .....
3. Điện thoại: .....
4. Fax: .....
5. Email: .....

II. Giới thiệu về hoạt động của tổ chức

1. Giới thiệu chung về hoạt động của tổ chức

(Cung cấp cho Cơ quan điều phối quốc gia các thông tin ngắn gọn giới thiệu về các lĩnh vực hoạt động của tổ chức, về năng lực ứng cứu sự cố của tổ chức như nhân sự, công nghệ, kinh nghiệm, đối tượng phục vụ,...)

.....
.....

2. Tên các hệ thống thông tin thuộc phụ trách quản lý hoặc hỗ trợ ứng cứu (cấp độ phê duyệt hoặc dự kiến tương đương):

▪ Cấp 1:	▪ Cấp 2:	▪ Cấp 3:	▪ Cấp 4:	▪ Cấp 5:
1.	1.	1.	1.	1.
2.	2.	2.	2.	2.
....	....	....	....	....

3. Thông tin về nhân lực, chuyên gia an toàn thông tin, công nghệ thông tin và tương đương

(Cung cấp thông về nhân lực, an toàn thông tin, công nghệ thông tin thuộc đơn vị mình theo bảng kèm theo Biểu mẫu 01 của Thông tư này)

III. Thông tin trao đổi, liên lạc trong mạng lưới

1. Địa chỉ Website:.....

2. Địa chỉ thư điện tử của đơn vị [1]:

PGP/GPG Public Key cho địa chỉ thư điện tử PoC của tổ chức: [2]

a) Tên (User ID) : .....
b) Fingerprint : .....
c) Liên kết đến Public key của tổ chức [3]: : .....

[1] *Địa chỉ thư điện tử được sử dụng làm đầu mối trao đổi thông tin với Mạng lưới ứng cứu sự cố, khuyến nghị không nên sử dụng địa chỉ thư điện tử cá nhân, nên sử dụng tên đại diện cho tổ chức.*
[2] *Nếu tổ chức chưa có thì có thể bỏ trống hoặc yêu cầu VNCERT hướng dẫn tạo.*
[3] *Tổ chức có thể gửi Public Key về VNCERT qua thư điện tử (csirts@vncert.vn).*

3. Đầu mối liên lạc trong giờ làm việc

a) Tên bộ phận/người giải quyết: .....

b) Điện thoại cố định: .....c) Điện thoại di động:.....

d) Số Fax:.....

4. Đầu mối liên lạc ngoài giờ làm việc

a) Tên bộ phận/người giải quyết: .....

b) Điện thoại cố định: .....c) Điện thoại di động:.....

d) Số Fax:.....

5. Đầu mối lãnh đạo phụ trách về an toàn thông tin của tổ chức [4]

a) Tên bộ phận/người giải quyết: .....

b) Điện thoại cố định: .....c) Điện thoại di động:.....

[4] *Đầu mối Lãnh đạo phụ trách về an toàn thông tin của tổ chức sẽ chỉ được sử dụng khi không liên lạc được với các đầu mối khác hoặc trong các tình huống sự cố có tính chất nghiêm trọng*

6. Địa chỉ nhận thư và công văn qua đường bưu điện:

a) Tên bộ phận/người nhận: .....

b) Vị trí, chức vụ:.....

c) Tên tổ chức:.....

d) Địa chỉ liên hệ: .....

đ) Điện thoại:.....

7. Phương tiện liên lạc khác [5]

Cách thức liên lạc khác qua hệ thống nhắn tin tức thời	
a) Yahoo ID:	
b) Skype:	
c) Google Talk:	
d) Hotmail:	
đ) Khác:	
[5] *Thông tin không bắt buộc*	

Chúng tôi cam kết tuân thủ các trách nhiệm, quyền hạn của thành viên mạng lưới, các quy định về hoạt động điều phối ứng cứu sự cố theo quy định pháp luật và hướng dẫn của Cơ quan điều phối quốc gia ban hành.

....., ngày..... tháng.....năm 20.....

NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT

(Ký tên và đóng dấu)

Mẫu số 03
Ban hành kèm theo Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông

BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO SỰ CỐ

- Tên tổ chức/cá nhân báo cáo sự cố (*) .....
- Địa chỉ: (*) .....
- Điện thoại (*) .....Email (*).....

NGƯỜI LIÊN HỆ

- Họ và tên (*) ..... Chức vụ:.....
- Điện thoại (*) .....Email (*).....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan*				
Phân loại cấp độ của hệ thống thông tin, (nếu có)	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):	*Điền tên nhà cung cấp ở đây*				
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*				
Dải địa chỉ Public IP kết nối với hệ thống bên ngoài:	*Điền thông tin ở đây*				

Mô tả sơ bộ về sự cố (*)
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:.....
.....
.....
.....
.....
.....
.....
.....

Ngày phát hiện sự cố (*) (dd/mm/yy)	/ /	Thời gian phát hiện (*):	.....giờ.... phút

HIỆN TRẠNG SỰ CỐ (*)

☐ Đã được xử lý ☐ Chưa được xử lý

CÁCH THỨC PHÁT HIỆN * *(Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*

☐ Qua hệ thống phát hiện xâm nhập ☐ Kiểm tra dữ liệu lưu lại (Log File)

☐ Nhận được thông báo từ: .....

☐ Khác, đó là .....

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

☐ Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân

☐ ISP đang trực tiếp cung cấp dịch vụ

☐ Cơ quan điều phối

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

- Hệ điều hành ..... Version .....
- Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*

  ☐ Web server ☐ Mail server ☐ Database server

  ☐ Dịch vụ khác, đó là .....
- Các biện pháp an toàn thông tin đã triển khai *(Đánh dấu những biện pháp đã triển khai)*

  ☐ Antivirus ☐ Firewall ☐ Hệ thống phát hiện xâm nhập

  ☐ Khác:.....
- Các địa chỉ IP của hệ thống *(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ)*

  .....
- Các tên miền của hệ thống

  .....
- Mục đích chính sử dụng hệ thống .....

  .....
- Thông tin gửi kèm

  ☐ Nhật ký hệ thống ☐ Mẫu virus / mã độc ☐ Khác:.....
- Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật: ☐ Có ☐ Không

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị
Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có).....

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ *: .../... /...../.../... (ngày/tháng/năm/giờ/phút)

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁT LUẬT
(Ký tên, đóng dấu)

Chú thích: *1. Phần (*) là những thông tin bắt buộc. Các phần còn lại có thể loại bỏ nếu không có thông tin.*

2. Sử dụng tiêu đề (subject) bắt đầu bằng "[TBSC]" khi gửi thông báo qua email

3. Tham khảo thêm tại website của VNCERT (www.vncert.gov.vn)

Mẫu số 04
Ban hành kèm theo Thông tư số /2017/TT-BTTTT ngày .../.../2017 của Bộ Thông tin và Truyền thông

BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

- Tên tổ chức/cá nhân báo cáo sự cố (*) .....
- Địa chỉ: (*) .....
- Điện thoại (*) .....Email (*) .....

KÝ HIỆU BÁO CÁO BAN ĐẦU SỰ CỐ: Số ký hiệu .... Ngày báo cáo: / / 201...

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*				
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*				
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố*				
Phân loại cấp độ của hệ thống thông tin, (nếu có)	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5

Tên/Mô tả về sự cố

Ngày phát hiện sự cố (*) (dd/mm/yy)	/ /	Thời gian phát hiện (*):	.....giờ.... phút

Kết quả xử lý sự cố
Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai...

Các tài liệu đính kèm
Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file...)

CÁ NHÂN/ NGƯỜI ĐẠI DIỆN THEO PHÁT LUẬT
(Ký tên, đóng dấu)

Mẫu số 05
Ban hành kèm theo Thông tư số 20/2017/TT-BTTTT ngày 12../9/2017 của Bộ Thông tin và Truyền thông

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Kính gửi: **Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam**

BÁO CÁO TỔNG HỢP [06 THÁNG/ 01 NĂM] VỀ HOẠT ĐỘNG TIẾP NHẬN VÀ XỬ LÝ SỰ CỐ

☐ Từ tháng ……../201 … đến tháng …./201…

Tên cơ quan/tổ chức: .....

Địa chỉ: .....

Mã thành viên mạng lưới: .....

1. Số lượng sự cố và cách thức xử lý

Loại sự cố/tấn công mạng	Số lượng	Số sự cố tự xử lý	Số sự cố có sự hỗ trợ xử lý từ các tổ chức khác	Số sự cố có hỗ trợ xử lý từ tổ chức nước ngoài	Số sự cố đề nghị VNCERT hỗ trợ xử lý	Thiệt hại ước tính
Từ chối dịch vụ						
Tấn công giả mạo						
Tấn công sử dụng mã độc						
Truy cập trái phép, chiếm quyền điều khiển						
Thay đổi giao diện						
Mã hóa phần mềm, dữ liệu, thiết bị						
Phá hoại thông tin, dữ liệu, phần mềm						
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 khác						
Tổng số						

2. Danh sách các tổ chức hỗ trợ xử lý sự cố

.....

3. Danh sách các tổ chức nước ngoài hỗ trợ xử lý sự cố

.....

4. Đề xuất kiến nghị: .....

.....

....., ngày ..... tháng ..... năm .....

NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT
(Đóng dấu hoặc sử dụng chữ ký số)

Mẫu số 06
Ban hành kèm theo Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM ỨNG CỨU
KHẨN CẤP MÁY TÍNH VIỆT NAM

Số: /VNCERT-NV
V/v Điều phối ứng cứu sự cố mạng

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

....., ngày..... tháng .... năm .....

Kính gửi: .....

Căn cứ chức năng nhiệm vụ theo thẩm quyền, trên cơ sở yêu cầu thực tế, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - VNCERT yêu cầu Quý cơ quan/đơn vị thực hiện lệnh/yêu cầu điều phối ứng cứu sự cố mạng dưới đây:

1. Loại yêu cầu điều phối

☐ Thông báo nguy cơ, tình hình sự cố và biện pháp phòng ngừa sự cố

☐ Yêu cầu xử lý sự cố cụ thể

☐ Yêu cầu xử lý kỹ thuật, thực hiện các biện pháp quản lý, kỹ thuật

☐ Yêu cầu báo cáo tình hình, cung cấp thông tin liên quan tới sự cố.

☐ Yêu cầu điều động nguồn lực (nhân lực, tài nguyên, công nghệ,...)

2. Tổ chức/hệ thống có liên quan tới sự cố

.....

.....

3. Nội dung cụ thể yêu cầu điều phối

.....

.....

.....

.....

.....

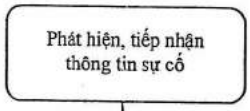
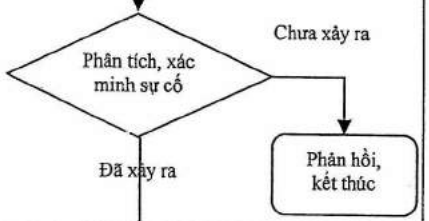
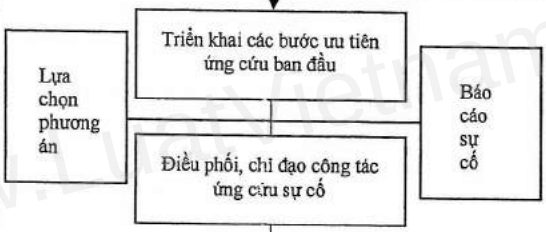
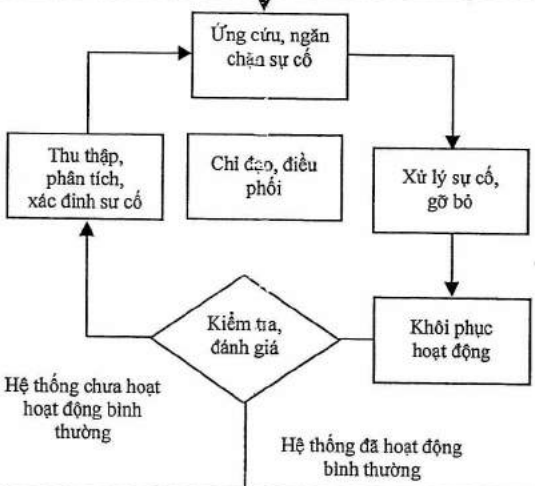
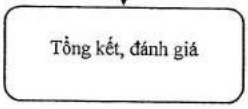
4. Thời hạn thực hiện yêu cầu điều phối đến ngày ...../...../.....

....., ngày ..... tháng ..... năm .....

GIÁM ĐỐC
(Đóng dấu hoặc sử dụng chữ ký số)

Phụ lục II
QUY TRÌNH ỨNG CỨU SỰ CỐ THÔNG THƯỜNG

(Ban hành kèm theo Thông tư số 20 /2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông)

Thành phần	Quy trình	Ghi chú
Đơn vị, cá nhân vận hành HTTT		Thông tin sự cố có thể từ các nguồn: - Hệ thống theo dõi nội bộ của đơn vị vận hành HTTT; - Đơn vị chuyên trách ƯCSC, Thông tin mạng lưới. - VNCERT - Nguồn tin xã hội
Đơn vị, cá nhân vận hành HTTT Đơn vị chuyên trách ứng cứu sự cố cùng cấp hoặc chịu trách nhiệm		Doanh nghiệp viễn thông, ISP; thành viên mạng lưới; Cơ quan điều phối quốc gia phối hợp hỗ trợ
- Đơn vị, cá nhân vận hành HTTT triển khai các bước ứng cứu ban đầu; báo cáo sự cố - Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh/Cơ quan điều phối quốc gia chỉ đạo, điều phối ứng cứu sự cố		Triển khai theo kế hoạch ứng phó sự cố đã được cấp thẩm quyền phê duyệt (nếu có) hoặc theo hướng dẫn của Đơn vị chuyên trách về ứng cứu sự cố hoặc Cơ quan điều phối quốc gia
- Đơn vị, cá nhân vận hành HTTT; Đơn vị chuyên trách/thành viên mạng lưới ứng cứu sự cố; Đội/bộ phận ứng cứu sự cố tổ chức triển khai phân tích, xác định nguồn gốc tấn công để tổ chức ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin - Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh/Cơ quan điều phối quốc gia chỉ đạo, điều phối ứng cứu sự cố		- Các thành phần tham gia ứng cứu sự cố căn cứu nội dung, nhiệm vụ được giao theo phân công, chỉ đạo tổ chức triển khai các quy trình, nghiệp vụ của mình. - Quy trình này được triển khai liên tục, đảm bảo đến khi khôi phụ hoạt động của hệ thống thông tin trở lại bình thường
Ban Chỉ đạo ứng cứu sự cố cấp bộ, tỉnh; Cơ quan điều phối quốc gia Đơn vị, cá nhân vận hành HTTT Đơn vị chuyên trách/thành viên mạng lưới ứng cứu sự cố liên quan Đội/bộ phận ứng cứu sự cố		

Phụ lục III

ĐỀ CƯƠNG KẾ HOẠCH ỨNG PHÓ SỰ CỐ AN TOÀN THÔNG TIN MẠNG

(Ban hành kèm theo Thông tư số 20 /2017/TT-BTTTT ngày 12/ 9 /2017 của Bộ trưởng Bộ Thông tin và Truyền thông)

1. Các quy định chung

a) Phạm vi và đối tượng của kế hoạch.

b) Điều kiện, nguyên tắc chung, nguyên tắc ưu tiên để duy trì hoạt động của hệ thống khi triển khai ứng cứu sự cố; phương châm ứng phó sự cố.

c) Các lực lượng tham gia ứng phó sự cố.

d) Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các cơ quan, đơn vị

- Đơn vị, cá nhân vận hành hệ thống thông tin;
- Nhà thầu cung cấp dịch vụ an toàn thông tin mạng (nếu có);
- Đơn vị chuyên trách ứng cứu sự cố;
- Đội ứng cứu sự cố;
- Ban chỉ đạo ứng cứu khẩn cấp sự cố cấp bộ, tỉnh;
- Cơ quan điều phối quốc gia;
- Cơ quan thường trực;
- Các đơn vị liên quan khác.

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

a) 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 thuộc phạm vi của kế hoạch;

b) 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;

c) Đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể có nếu xảy ra sự cố;

d) 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).

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 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) Quy trình triển khai và các bước ưu tiên ứng cứu ban đầu khi hệ thống thông tin gặp sự cố, có phân theo các loại sự cố.

b) 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....

c) 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....

d) 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;

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.

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

a) Triển khai các hoạt động thuộc trách nhiệm của các cơ quan, đơn vị liên quan theo quy định tại các Điều 9 đến Điều 11 và các nội dung liên quan khác của Thông tư này;

b) 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.

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 tại Mục 4;

- 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.

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.

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

- Mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố;

- Chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, 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, bộ phận 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.

6. Các giải pháp đảm bảo, tổ chức triển khai kế hoạch và kinh phí

a) Các giải pháp để thực hiện kế hoạch;

b) Nguồn lực và điều kiện bảo đảm thực hiện kế hoạch;

c) Kinh phí và nguồn vốn triển khai thực hiện kế hoạch;

d) Phân công tổ chức thực hiện.

Các nội dung, nhiệm vụ trong kế hoạch này có thể triển khai theo hình thức tự thực hiện hoặc thuê nhà thầu cung cấp dịch vụ để triển khai, hoặc có thể kết hợp cả 2 hình thức./.