THỦ TƯỚNG CHÍNH PHỦ

THỦ TƯỚNG CHÍNH PHỦ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 05/2017/QĐ-TTg	*Hà Nội, ngày 16 tháng 3 năm 2017*

QUYẾT ĐỊNH
Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

Căn cứ Luật tổ chức Chính phủ ngày 19 tháng 6 năm 2015;

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 về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Theo đề nghị của Bộ trưởng Bộ Thông tin và Truyền thông;

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.

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi áp dụng

Quyết định này quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

Hệ thống thông tin do Bộ Quốc phòng, Bộ Công an quản lý không thuộc phạm vi điều chỉnh của Quyết định này.

Điều 2. Đối tượng áp dụng

Quyết định này áp dụng đối với các cơ quan, tổ chức, doanh nghiệp, cá nhân trực tiếp tham gia hoặc có liên quan đến hoạt động ứng cứu sự cố bảo đảm an toàn thông tin mạng tại Việt Nam.

Chương II
PHÂN CẤP TỔ CHỨC THỰC HIỆN ỨNG CỨU SỰ CỐ BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG QUỐC GIA

Điều 3. Ban Chỉ đạo quốc gia về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng

1. Ban Chỉ đạo an toàn thông tin quốc gia đảm nhiệm chức năng Ban Chỉ đạo quốc gia về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng (sau đây gọi là Ban Chỉ đạo quốc gia).

2. Ban Chỉ đạo quốc gia có trách nhiệm chỉ đạo Bộ Thông tin và Truyền thông, Bộ Công an, Bộ Quốc phòng và các bộ, ngành, địa phương liên quan trong công tác ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia.

Điều 4. Cơ quan thường trực về ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

1. Bộ Thông tin và Truyền thông là cơ quan thường trực, giúp việc cho Ban Chỉ đạo quốc gia (sau đây gọi là Cơ quan thường trực) có nhiệm vụ, quyền hạn cụ thể sau:

a) Quyết định lựa chọn phương án ứng cứu và chủ trì, chỉ đạo công tác ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

b) Chỉ đạo Cơ quan điều phối quốc gia tiếp nhận, thu thập, xử lý thông tin, báo cáo về sự cố mất an toàn thông tin mạng quốc gia và đề xuất phương án ứng cứu;

c) Triệu tập, chỉ đạo Bộ phận tác nghiệp ứng cứu sự cố an toàn thông tin mạng quốc gia theo đề xuất của Cơ quan điều phối quốc gia; chỉ đạo, phân công nhiệm vụ cho các đơn vị chuyên trách về ứng cứu sự cố, các thành viên mạng lưới ứng cứu để triển khai phương án ứng cứu;

d) Làm đầu mối hoặc chỉ định Cơ quan điều phối làm đầu mối quốc gia phối hợp với các đơn vị chức năng của các quốc gia khác hoặc các tổ chức quốc tế trong hoạt động ứng cứu, xử lý các sự cố liên quốc gia;

đ) Kiểm tra, giám sát, đôn đốc việc chấp hành của các đơn vị liên quan, báo cáo Ban Chỉ đạo quốc gia về công tác ứng cứu khẩn cấp sự cố an toàn thông tin mạng quốc gia.

2. Trường hợp cần thiết, Bộ Thông tin và Truyền thông chủ trì thành lập 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), với thành phần gồm: 01 lãnh đạo Bộ Thông tin và Truyền thông làm Trưởng ban, Cơ quan điều phối quốc gia làm thường trực và thành viên là các lãnh đạo cấp Cục, Vụ của một số bộ ngành, tổ chức có liên quan.

Điều 5. 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

1. Ban Chỉ đạo ứng dụng công nghệ thông tin 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 đảm nhiệm chức năng Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng trong phạm vi địa bàn, lĩnh vực mình phụ trách (sau đây gọi là Ban Chỉ đạo cấp bộ, tỉnh).

Trong trường hợp chưa có Ban Chỉ đạo ứng dụng công nghệ thông tin hoặc điều kiện đặc thù cần thiết, bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh xem xét thành lập Ban Chỉ đạo ứng cứu khẩn cấp sự cố an toàn thông tin mạng trong phạm vi bộ, ngành, địa phương mình do 1 lãnh đạo bộ hoặc lãnh đạo Ủy ban nhân dân cấp tỉnh trực tiếp chỉ đạo.

2. Trách nhiệm, quyền hạn của Ban chỉ đạo cấp bộ, tỉnh:

a) Chỉ đạo công tác điều phối, ứng cứu sự cố trong phạm vi ngành, lĩnh vực, địa phương mình; 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;

b) Triệu tập, chỉ đạo Đội ứng cứu sự cố hoặc Bộ phận tác nghiệp ứng cứu sự cố an toàn thông tin mạng cùng cấp theo đề xuất của đơn vị chuyên trách ứng cứu sự cố;

c) Báo cáo tình hình và xin ý kiến của Ban Chỉ đạo quốc gia qua Cơ quan thường trực về các vấn đề phát sinh vượt thẩm quyền trong quá trình thực hiện nhiệm vụ; chịu sự chỉ đạo, điều hành của Ban Chỉ đạo quốc gia qua Cơ quan thường trực và Cơ quan điều phối quốc gia.

Điều 6. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng

1. Đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng là Cơ quan chuyên trách về an toàn thông tin hoặc cơ quan chuyên trách về công nghệ thông tin của các bộ, ngành, Ủy ban nhân dân cấp tỉnh (sau đây gọi tắt là Đơn vị chuyên trách ứng cứu sự cố).

Các doanh nghiệp viễn thông, Internet, các cơ quan, tổ chức, doanh nghiệp chủ quản hệ thống thông tin lớn thành lập hoặc chỉ định đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng tại cơ quan, tổ chức mình.

2. Đơn vị chuyên trách ứng cứu sự cố có trách nhiệm trình thành lập Đội ứng cứu sự cố và tổ chức hoạt động ứng cứu sự cố trong lĩnh vực, địa bàn, phạm vi mình quản lý; 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.

Điều 7. Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia

1. Thành viên có nghĩa vụ phải tham gia mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia (sau đây gọi tắt là mạng lưới ứng cứu sự cố) gồm:

a) Đơn vị chuyên trách về ứng cứu sự cố, an toàn thông tin hoặc công nghệ thông tin của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, cơ quan trung ương; Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;

b) Cơ quan, đơn vị có chức năng liên quan thuộc Bộ Thông tin và Truyền thông: Cục An toàn thông tin, Trung tâm Ứng cứu khẩn cấp máy tính Việt nam (VNCERT), Trung tâm Internet Việt Nam (VNNIC), Cục Bưu điện Trung ương;

c) Cơ quan, đơn vị có chức năng liên quan thuộc Bộ Công an: Cục An ninh mạng; Cục Cảnh sát phòng, chống tội phạm sử dụng công nghệ cao;

d) Cơ quan, đơn vị có chức năng liên quan thuộc Bộ Quốc phòng: Cục Công nghệ thông tin; Ban Cơ yếu Chính phủ;

đ) Các doanh nghiệp cung cấp dịch vụ hạ tầng viễn thông, Internet (ISP); các tổ chức, doanh nghiệp cung cấp dịch vụ trung tâm dữ liệu, cho thuê không gian lưu trữ thông tin số; đơn vị quản lý, vận hành cơ sở dữ liệu quốc gia; đơn vị chuyên trách về an toàn thông tin, công nghệ thông tin của các tổ chức ngân hàng, tài chính, kho bạc, thuế, hải quan;

e) Các tổ chức, doanh nghiệp quản lý, vận hành các hệ thống thông tin quan trọng, các hệ thống điều khiển công nghiệp (SCADA) thuộc các lĩnh vực: Năng lượng, công nghiệp, y tế, tài nguyên và môi trường, giáo dục và đào tạo, dân cư và đô thị.

2. Thành viên tự nguyện tham gia mạng lưới: Là các tổ chức, doanh nghiệp không thuộc danh sách quy định tại khoản 1 Điều này, có năng lực về an toàn thông tin hoặc công nghệ thông tin, có đăng ký và được Cơ quan điều phối quốc gia chấp thuận tham gia mạng lưới. Khuyến khích các tổ chức, doanh nghiệp hoạt động trong lĩnh vực an toàn thông tin, công nghệ thông tin; các tổ chức, doanh nghiệp quản lý, vận hành hệ thống thông tin quy mô lớn, hệ thống thông tin chuyên ngành ngân hàng, tài chính, hệ thống điều khiển công nghiệp (SCADA); và các đơn vị khác có năng lực về an toàn thông tin đăng ký tham gia mạng lưới.

3. Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (Trung tâm VNCERT) là Cơ quan điều phối quốc gia về ứng cứu sự cố (gọi tắt là Cơ quan điều phối quốc gia hay Cơ quan điều phối), có trách nhiệm:

a) Thực hiện chức năng điều phối các hoạt động 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 tại Việt Nam; có quyền quyết định hình thức điều phối các hoạt động ứng cứu sự cố và chịu trách nhiệm về các lệnh/yêu cầu điều phối;

b) Chủ trì xây dựng quy chế hoạt động của mạng lưới; tổ chức và điều hành hoạt động của mạng lưới; tổng hợp và chia sẻ thông tin, cảnh báo sự cố trong mạng lưới; đề xuất và tiếp nhận, quản lý các khoản đóng góp, tài trợ của các thành viên và các tổ chức, cá nhân và nguồn thu hợp pháp khác để chi cho các hoạt động của mạng lưới; là đầu mối quốc gia hợp tác với các tổ chức, doanh nghiệp nước ngoài trong công tác ứng cứu sự cố bảo đảm an toàn thông tin mạng;

c) Bộ Thông tin và Truyền thông thành lập Ban điều hành mạng lưới do lãnh đạo Cơ quan điều phối làm trưởng ban, thành viên là đại diện lãnh đạo một số thành viên mạng lưới để điều hành, phối hợp và tổ chức các hoạt động cho mạng lưới.

4. Các thành viên mạng lưới có trách nhiệm tuân thủ quy chế hoạt động của mạng lưới, tuân thủ các yêu cầu điều phối của cơ quan điều phối, tham gia, đóng góp tích cực cho hoạt động của mạng lưới. Doanh nghiệp viễn thông, nhà cung cấp dịch vụ Internet ISP có trách nhiệm lưu trữ và cung cấp thông tin liên quan đến các địa chỉ IP thuê bao, máy chủ, thiết bị IOT, các log file, nhật ký dịch vụ phân giải tên miền DNS trong phạm vi quản lý của doanh nghiệp; thiết lập môi trường để lắp đặt thiết bị quan trắc, lấy mẫu và cung cấp luồng dữ liệu mạng để phục vụ giám sát, phát hiện sự cố theo yêu cầu của cơ quan điều phối quốc gia; thiết lập đầu mối thường trực 24/7, bố trí nhân, vật lực sẵn sàng phối hợp, triển khai các giải pháp nhằm ứng cứu, khắc phục hậu quả sự cố trong trường hợp nguồn tấn công được xác định xuất phát từ thuê bao thuộc doanh nghiệp mình hoặc khi được yêu cầu từ cơ quan điều phối quốc gia.

Điều 8. Bộ phận tác nghiệp ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

1. Bộ phận tác nghiệp ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia (sau đây gọi tắt là Bộ phận tác nghiệp ứng cứu khẩn cấp) do Cơ quan thường trực triệu tập và chịu sự điều hành của Cơ quan thường trực với sự tham gia của các đơn vị sau:

a) Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam VNCERT - thường trực);

b) Cục An toàn thông tin, Bộ Thông tin và Truyền thông;

c) Cục An ninh mạng, Cục Cảnh sát phòng, chống tội phạm sử dụng công nghệ cao - Bộ Công an;

d) Cục Công nghệ thông tin, Bộ Tổng tham mưu, Bộ Quốc phòng;

đ) Một số đơn vị chuyên trách về ứng cứu sự cố an toàn thông tin mạng của các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân cấp tỉnh, doanh nghiệp viễn thông, Internet, chủ quản hệ thống thông tin quan trọng quốc gia.

2. Quyền hạn của Bộ phận tác nghiệp ứng cứu khẩn cấp

a) Sử dụng các biện pháp nghiệp vụ, trang thiết bị, phương tiện kỹ thuật và các biện pháp khác theo chức năng nhiệm vụ được giao và tuân thủ quy định của pháp luật;

b) Yêu cầu cơ quan, tổ chức, cá nhân cung cấp thông tin, tài liệu, thiết bị khi có căn cứ xác định liên quan đến sự cố nhằm phục vụ hoạt động ứng cứu;

c) Kiểm tra hệ thống thông tin của cơ quan, tổ chức, cá nhân khi có căn cứ xác định liên quan đến sự cố nhằm phục vụ hoạt động ứng cứu;

d) Yêu cầu cơ quan, tổ chức, doanh nghiệp viễn thông, Internet có liên quan phối hợp thực hiện các công việc cần thiết cho hoạt động ứng cứu, khắc phục sự cố.

3. Cơ chế phối hợp và chia sẻ thông tin giữa các đơn vị tham gia bộ phận tác nghiệp ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia theo quy định của pháp luật và quyết định của Thủ tướng Chính phủ.

Chương III
PHƯƠNG ÁN ỨNG CỨU

Điều 9. Phân nhóm sự cố an toàn thông tin mạng

Sự cố an toàn thông tin mạng nghiêm trọng là sự cố đáp ứng đồng thời các tiêu chí sau:

1. Hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 4, cấp độ 5 hoặc thuộc Danh mục hệ thống thông tin quan trọng quốc gia và bị một trong số các sự cố sau:

a) Hệ thống bị gián đoạn dịch vụ;

b) Dữ liệu tuyệt mật hoặc bí mật nhà nước có khả năng bị tiết lộ;

c) Dữ liệu quan trọng của hệ thống không bảo đảm tính toàn vẹn và không có khả năng khôi phục được;

d) Hệ thống bị mất quyền điều khiển;

đ) Sự cố có khả năng xảy ra trên diện rộng hoặc gây ra các ảnh hưởng dây chuyền, làm tổn hại cho các hệ thống thông tin cấp độ 4 hoặc cấp độ 5 khác.

2. Chủ quản hệ thống thông tin không đủ khả năng tự kiểm soát, xử lý được sự cố.

Điều 10. Hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

1. Phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia là phương án ứng cứu cho sự cố an toàn thông tin mạng nghiêm trọng đáp ứng các tiêu chí tại Điều 9 và hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 5 hoặc thuộc Danh mục Hệ thống thông tin quan trọng quốc gia.

2. Phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng của cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội là phương án ứng cứu cho sự cố an toàn thông tin mạng nghiêm trọng đáp ứng các tiêu chí tại Điều 9, hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 4 và chủ quản hệ thống thông tin thuộc các bộ, cơ quan ngang bộ, cơ quan thuộc Chính phủ và các cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội ở trung ương (gọi chung là cơ quan trung ương).

3. Phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng của địa phương là phương án ứng cứu cho sự cố an toàn thông tin mạng nghiêm trọng đáp ứng các tiêu chí tại Điều 9, hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 4 và chủ

quản hệ thống thông tin thuộc Ủy ban nhân dân hoặc Tỉnh ủy, Thành ủy các tỉnh, thành phố trực thuộc Trung ương quản lý (gọi chung là cơ quan địa phương).

4. Phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng của doanh nghiệp là phương án ứng cứu cho sự cố an toàn thông tin mạng nghiêm trọng đáp ứng các tiêu chí tại Điều 9, hệ thống thông tin bị sự cố là hệ thống thông tin cấp độ 4 và chủ quản hệ thống thông tin là doanh nghiệp viễn thông, doanh nghiệp nhà nước có quản lý các hệ thống thông tin từ cấp độ 4 trở lên, hoặc tổ chức, doanh nghiệp có quản lý hệ thống thông tin thuộc Danh mục Hệ thống thông tin quan trọng quốc gia (sau đây gọi chung là doanh nghiệp quản lý hạ tầng thông tin quan trọng).

Điều 11. Báo cáo sự cố an toàn thông tin mạng

1. Báo cáo sự cố an toàn thông tin mạng:

a) Đơn vị vận hành hệ thống thông tin có trách nhiệm báo cáo sự cố tới cơ quan chủ quản, đơn vị chuyên trách ứng cứu sự cố cùng cấp, Cơ quan điều phối quốc gia chậm nhất 5 ngày kể từ khi phát hiện sự cố; trường hợp xác định sự cố có thể vượt khả năng xử lý của mình, đơn vị vận hành hệ thống thông tin phải thực hiện quy trình báo cáo khẩn cấp theo quy định tại khoản 2 đến khoản 5 Điều này ngay khi phát hiện sự cố hoặc xác định sự cố có thể vượt khả năng xử lý của mình;

b) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng thông báo cho đơn vị vận hành hệ thống thông tin, cơ quan chủ quản hệ thống thông tin liên quan, cơ quan điều phối quốc gia và đơn vị chuyên trách ứng cứu sự cố hoặc thành viên mạng lưới ứng cứu sự cố có trách nhiệm liên quan.

2. Báo cáo sự cố phải được thực hiện ngay lập tức và được duy trì trong suốt quá trình ứng cứu sự cố gồm: Báo cáo ban đầu; báo cáo diễn biến tình hình; báo cáo phương án ứng cứu cụ thể; báo cáo xin ý kiến chỉ đạo, chỉ huy; báo cáo đề nghị hỗ trợ, phối hợp; báo cáo kết thúc ứng phó.

3. Hình thức báo cáo bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện hoặc thông qua hệ thống báo cáo, cảnh báo sự cố an toàn mạng quốc gia; mẫu báo cáo theo quy định về điều phối ứng cứu, hoặc theo hướng dẫn của cơ quan điều phối quốc gia.

4. Nội dung báo cáo ban đầu gồm:

a) Tên, địa chỉ Đơn vị vận hành hệ thống thông tin; cơ quan chủ quản hệ thống thông tin; hệ thống thông tin bị sự cố; thời điểm phát hiện sự cố;

b) Đầu mối liên lạc về sự cố của đơn vị vận hành hệ thống bị sự cố: Tên, chức vụ, điện thoại, thư điện tử;

c) Mô tả về sự cố: Loại sự cố, hiện tượng, đánh giá sơ bộ mức độ nguy hại, mức độ lây lan, tác động của sự cố đến hoạt động bình thường của tổ chức;

d) Đơn vị cung cấp dịch vụ hạ tầng công nghệ thông tin, viễn thông;

đ) Liệt kê các biện pháp đã triển khai hoặc dự kiến triển khai để xử lý khắc phục sự cố;

e) Các tổ chức, doanh nghiệp đang hỗ trợ ứng cứu, xử lý và kết quả xử lý sự cố tính đến thời điểm báo cáo;

g) Kết quả ứng cứu sự cố ban đầu;

h) Kiến nghị đề xuất hướng ứng cứu xử lý sự cố (nếu có).

5. Nguyên tắc báo cáo, trao đổi thông tin trong ứng cứu sự cố:

a) Đơn vị vận hành hệ thống thông tin báo cáo Chủ quản hệ thống thông tin, đơn vị chuyên trách ứng cứu sự cố cùng cấp, đồng gửi Cơ quan điều phối quốc gia;

b) Đơn vị chuyên trách ứng cứu sự cố báo cáo Chủ quản hệ thống thông tin, Ban Chỉ đạo cấp trên trực tiếp và Cơ quan điều phối quốc gia;

c) Ban Chỉ đạo cấp bộ, tỉnh và cơ quan điều phối quốc gia báo cáo Cơ quan thường trực và Ban Chỉ đạo quốc gia.

Điều 12. Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng

1. Đơn vị chuyên trách về ứng cứu sự cố hoặc thành viên mạng lưới ứng cứu sự cố, khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố an toàn thông tin mạng trong phạm vi mình chịu trách nhiệm phải thực hiện:

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

b) Thông báo ngay thông tin sự cố đến Cơ quan điều phối quốc gia, đơn vị vận hành hệ thống thông tin, cơ quan chủ quản hệ thống thông tin và các cơ quan chức năng liên quan;

c) 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;

d) Thẩm tra, xác minh và phân loại sự cố an toàn thông tin mạng để lựa chọn phương án ứng cứu phù hợp hoặc đề xuất với Ban chỉ đạo cấp trên trực tiếp và cơ quan điều phối quốc gia trong trường hợp vượt thẩm quyền;

đ) Chủ động hỗ trợ đơn vị vận hành hệ thống thông tin ứng cứu, xử lý sự cố trong khả năng và trách nhiệm của mình;

e) Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo Ban Chỉ đạo cấp trên trực tiếp 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;

g) Tổng hợp báo cáo Cơ quan điều phối quốc gia theo định kỳ 6 tháng một lần và báo cáo đột xuất khi được yêu cầu.

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

a) Công khai trên trang tin điện tử của mình số điện thoại, số fax và email đường dây nóng và bảo đảm nguồn lực để duy trì trực đường dây nóng liên tục để kịp thời tiếp nhận và xử lý sự cố;

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

c) 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;

d) Cung cấp đầu mối liên lạc riêng đối với sự cố nghiêm trọng;

đ) 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 quyết định sự cố nghiêm trọng và phương án ứng cứu khẩn cấp phù hợp; báo cáo, đề xuất với Cơ quan thường trực và Ban Chỉ đạo quốc gia các vấn đề vượt thẩm quyền;

e) 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;

g) Thực hiện các trách nhiệm khác của Cơ quan điều phối quốc gia.

3. Đơn vị vận hành hệ thống thông tin khi phát hiện hoặc nhận được thông báo sự cố đối với hệ thống thông tin do mình quản lý, phải thực hiện:

a) Ghi nhận, tiếp nhận thông báo, báo cáo sự cố và tập hợp các thông tin liên quan theo đúng quy trình;

b) 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;

c) Chủ trì, phối hợp cùng đơn vị cung cấp dịch vụ an toàn thông tin mạng (nếu có) và các đơn vị chức năng liên quan tiến hành phân tích, xác minh, đánh giá tình hình, sơ bộ phân loại sự cố và triển khai ngay các hoạt động ứng cứu sự cố và báo cáo theo quy định;

d) Báo cáo về sự cố, diễn biến tình hình ứng cứu sự cố, đề xuất hỗ trợ ứng cứu sự cố hoặc nâng cấp nghiêm trọng của sự cố (khi cần) cho chủ quản hệ thống thông tin, Cơ quan điều phối quốc gia và đơn vị chuyên trách ứng cứu sự cố cùng cấp.

Điều 13. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường

Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường theo các văn bản hướng dẫn, quy định của Bộ Thông tin và Truyền thông và Cơ quan điều phối quốc gia.

Điều 14. Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng

Quy trình ứng cứu khẩn cấp sự cố an toàn thông tin mạng nghiêm trọng sau đây được sử dụng chung cho cả bốn phương án ứng cứu khẩn cấp nêu trong Điều 10 Quyết định này, cụ thể bao gồm các bước sau:

1. Phát hiện hoặc tiếp nhận sự cố

Đơn vị chủ trì: Đơn vị vận hành hệ thống thông tin; Cơ quan điều phối quốc gia.

Đơn vị phối hợp: Đơn vị chuyên trách về ứng cứu sự cố; Chủ quản hệ thống thông tin.

Nội dung thực hiện: Đơn vị vận hành hệ thống thông tin chịu trách nhiệm liên tục theo dõi, phát hiện các tấn công, sự cố đối với hệ thống mình được giao quản lý, vận hành. Cơ quan điều phối quốc gia là đơn vị đầu mối tổ chức các hoạt động theo dõi, giám sát, phát hiện các sự cố và tiếp nhận thông báo về sự cố an toàn thông tin mạng từ các nguồn khác nhau.

2. Xác minh, phân tích, đánh giá và phân loại sự cố

Đơn vị chủ trì: Cơ quan điều phối quốc gia.

Đơn vị phối hợp: Chủ quản hệ thống thông tin; Đơn vị chuyên trách về ứng cứu sự cố; Đơn vị vận hành hệ thống thông tin.

Nội dung thực hiện:

a) Cơ quan điều phối quốc gia phối hợp cùng chủ quản hệ thống thông tin (hoặc đơn vị được ủy quyền như đơn vị chuyên trách về ứng cứu sự cố hoặc đơn vị vận hành hệ thống thông tin) xác minh sự cố bao gồm các thông tin sau: Tình trạng sự cố; mức độ sự cố; phạm vi ảnh hưởng của sự cố; đối tượng, địa điểm xảy ra sự cố;

b) Sau khi xác minh được sự cố, Cơ quan điều phối quốc gia có trách nhiệm phân loại sự cố và triển khai tiếp như sau:

- Trường hợp sự cố được phân loại thông thường (không đạt các tiêu chí quy định tại Điều 9 Quyết định này) thì Cơ quan điều phối quốc gia thông 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;

- Trường hợp sự cố được phân loại nghiêm trọng (đạt các tiêu chí quy định tại Điều 9 Quyết định này) thì Cơ quan điều phối quốc gia báo cáo Cơ quan thường trực về sự cố nghiêm trọng cùng với các đề xuất: Phương án ứng cứu; 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 theo khoản 3 Điều này.

3. Cơ quan thường trực quyết định lựa chọn phương án và triệu tập các thành viên của bộ phận tác nghiệp ứng cứu khẩn cấp.

Đơn vị chủ trì: Cơ quan thường trực.

Nội dung thực hiện:

a) Cơ quan thường trực căn cứ theo báo cáo của Cơ quan điều phối quốc gia xem xét quyết định lựa chọn phương án ứng cứu khẩn cấp quốc gia và triệu tập bộ phận tác nghiệp ứng cứu khẩn cấp để ứng cứu, xử lý sự cố. Tùy theo tình hình thực tế, bộ phận tác nghiệp ứng cứu khẩn cấp được huy động từ số các đơn vị theo quy định tại Điều 8 Quyết định này phù hợp với phương án ứng cứu được lựa chọn và đặc thù của sự cố;

b) Nguyên tắc phân công nhiệm vụ triển khai các biện pháp ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia như sau:

- Chỉ đạo điều hành hoạt động ứng cứu và giám sát cơ chế phối hợp, chia sẻ thông tin: Bộ Thông tin và Truyền thông, Ban điều phối ứng cứu quốc gia;

- Thu thập, tổng hợp thông tin và chia sẻ, báo cáo: Cơ quan điều phối quốc gia, chủ quản hệ thống thông tin (qua đơn vị vận hành hệ thống thông tin và đơn vị chuyên trách ứng cứu sự cố);

- Phân tích thông tin: Cơ quan điều phối quốc gia, đơn vị vận hành hệ thống thông tin, đơn vị chuyên trách ứng cứu sự cố và các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp;

- Ngăn chặn, xử lý sự cố: Đơn vị vận hành hệ thống thông tin, đơn vị chuyên trách ứng cứu sự cố, Cơ quan điều phối quốc gia và các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp;

- Khắc phục, gỡ bỏ, khôi phục dữ liệu và hoạt động bình thường: Chủ quản hệ thống thông tin, các đơn vị được chủ quản hệ thống thông tin lựa chọn;

- Xử lý hậu quả: Chủ quản hệ thống thông tin, các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp;

- Công bố và xử lý khủng hoảng thông tin: Cơ quan thường trực, Cơ quan điều phối quốc gia.

4. Triển khai phương án ứng cứu ban đầu

Đơn vị chủ trì: Cơ quan điều phối quốc gia, Chủ quản hệ thống thông tin.

Nội dung thực hiện: Cơ quan điều phối quốc gia nhanh chóng phối hợp với chủ quản hệ thống thông tin tiến hành ngay các biện pháp ứng cứu ban đầu, bao gồm:

a) Xác định phạm vi, đối tượng, mục tiêu cần ứng cứu:

- Các sự cố liên quan đã xảy ra;

- Đối tượng đang bị ảnh hưởng;

- Phạm vi bị ảnh hưởng;

- Các mục tiêu ưu tiên trong khắc phục sự cố (khôi phục hoạt động, bảo đảm bí mật dữ liệu; bảo đảm tính toàn vẹn dữ liệu);

- Diễn biến tình hình và phương thức thủ đoạn tấn công;

- Dự đoán các diễn biến tiếp theo có thể xảy ra.

b) Điều phối các hoạt động ứng cứu ban đầu: Cơ quan thường trực chỉ đạo Cơ quan điều phối quốc gia thực hiện điều phối và chia sẻ thông tin, tài liệu liên quan đến tình huống ứng cứu cho các thành viên tham gia theo chức năng, nhiệm vụ được giao;

c) Cảnh báo sự cố trên mạng lưới ứng cứu quốc gia: Cơ quan điều phối quốc gia thực hiện cảnh báo cho các thành viên mạng lưới và các đối tượng có liên quan hoặc có khả năng xảy ra các sự cố tương tự;

d) Tiến hành các biện pháp khôi phục tạm thời:

Căn cứ vào mục tiêu được ưu tiên trong khắc phục sự cố, Chủ quản hệ thống thông tin phối hợp với Cơ quan điều phối quốc gia, các nhà cung cấp dịch vụ và các cơ quan chức năng khác tiến hành khôi phục một số hoạt động, dữ liệu hoặc kết nối cần thiết nhất để giảm thiểu thiệt hại đối với hệ thống thông tin, ảnh hưởng uy tín của cơ quan chủ quản, quản lý hệ thống hoặc gây ảnh hưởng xấu tới xã hội.

Chủ quản hệ thống thông tin phải phối hợp chặt chẽ, cung cấp đầy đủ thông tin để Cơ quan điều phối quốc gia thực hiện giám sát, theo dõi quá trình phục hồi và các tấn công, ảnh hưởng trong thời gian chưa khắc phục triệt để sự cố;

đ) Xử lý hậu quả ban đầu: Chủ quản hệ thống thông tin cần nhanh chóng tiến hành các biện pháp khắc phục khẩn cấp các hậu quả, thiệt hại do tấn công mạng gây ra làm ảnh hưởng đến người dân, xã hội, cơ quan, tổ chức khác theo yêu cầu của Cơ quan thường trực;

e) Ngăn chặn, xử lý các hành vi đã được phát hiện: Cơ quan thường trực điều phối hoặc chỉ đạo Cơ quan điều phối quốc gia thực hiện điều phối các cơ quan chức năng triển khai hỗ trợ phát hiện và xử lý các nguồn phát tán tấn công, ngăn chặn các tấn công từ bên ngoài vào hệ thống thông tin bị sự cố. Cơ quan thường trực cung cấp hoặc chỉ đạo cung cấp các thông tin, chứng cứ liên quan đến các hành vi vi phạm pháp luật có yếu tố cấu thành tội phạm (nếu có) để các cơ quan chức năng thuộc Bộ Công an tiến hành điều tra, xác minh và ngăn chặn tội phạm.

5. Triển khai phương án ứng cứu khẩn cấp

a) Chỉ đạo xử lý sự cố

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

Nội dung thực hiện: Căn cứ theo phương án ứng cứu được lựa chọn, Cơ quan thường trực chỉ đạo chủ quản hệ thống thông tin, Cơ quan điều phối quốc gia, bộ phận tác nghiệp ứng cứu sự cố triển khai công tác ứng cứu, xử lý sự cố. Trong quá trình ứng cứu, tùy thuộc vào diễn biến tình hình thực tế, Cơ quan thường trực có thể quyết định bổ sung thành phần tham gia tác nghiệp ứng cứu khẩn cấp;

b) Điều phối công tác ứng cứu

Đơn vị chủ trì: Ban điều phối ứng cứu quốc gia, Cơ quan điều phối quốc gia.

Nội dung thực hiện: Căn cứ theo phương án ứng cứu được lựa chọn, Ban Điều phối ứng cứu quốc gia hoặc Cơ quan điều phối quốc gia thực hiện công tác điều phối ứng cứu theo chức năng nhiệm vụ của mình và giám sát cơ chế phối hợp, chia sẻ thông tin;

c) Phát ngôn và công bố thông tin

Cơ quan thường trực chịu trách nhiệm chỉ định người phát ngôn, cung cấp thông tin; quyết định địa điểm, nội dung, thời điểm phát ngôn, cung cấp thông tin cho các cơ quan thông tin đại chúng, các cá nhân và tổ chức có liên quan đến sự cố;

d) Thu thập thông tin

Đơn vị chủ trì: Cơ quan điều phối quốc gia, chủ quản hệ thống thông tin.

Nội dung thực hiện: Căn cứ theo yêu cầu cung cấp thông tin cho các đơn vị thuộc thành phần tác nghiệp ứng cứu khẩn cấp, cơ quan điều phối quốc gia cùng chủ quản hệ thống thông tin phối hợp tiến hành thu thập, tổng hợp và chia sẻ, cung cấp thông tin;

đ) Phân tích, giám sát tình hình liên quan sự cố

Cơ quan điều phối quốc gia chủ trì, phối hợp với chủ quản hệ thống thông tin thực hiện giám sát liên tục diễn biến sự cố và thông báo, cập nhật đến các đơn vị trong bộ phận tác nghiệp ứng cứu khẩn cấp.

Các đơn vị thuộc bộ phận tác nghiệp ứng cứu khẩn cấp dựa trên các thông tin thu thập được, sử dụng các nguồn lực, phương tiện và các quy trình nghiệp vụ của mình để tiến hành phân tích sự cố. Kết quả phân tích sự cố được báo cáo Cơ quan thường trực, Cơ quan điều phối quốc gia và chia sẻ trong bộ phận tác nghiệp ứng cứu khẩn cấp để phục vụ ứng cứu, khắc phục sự cố;

e) Khắc phục sự cố, gỡ bỏ mã độc

Đơn vị chủ trì: Chủ quản hệ thống thông tin.

Đơn vị phối hợp: Cơ quan điều phối quốc gia, các đơn vị khác thuộc Bộ phận tác nghiệp ứng cứu khẩn cấp.

Nội dung thực hiện:

- Sao lưu hệ thống trước và sau khi xử lý sự cố;
- Tiêu diệt các mã độc, phần mềm độc hại;
- Khôi phục hệ thống, dữ liệu và kết nối;
- Cấu hình hệ thống an toàn;
- Kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố;
- Khắc phục các điểm yếu an toàn thông tin;

- Bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin cho hệ thống;

- Triển khai theo dõi, giám sát, ngăn chặn khả năng lặp lại sự cố hoặc xảy ra các sự cố tương tự.

g) Ngăn chặn, xử lý hậu quả

Chủ quản hệ thống thông tin có trách nhiệm xử lý các hậu quả do sự cố hệ thống thông tin của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác.

Các đơn vị thuộc thành phần tham gia tác nghiệp ứng cứu khẩn cấp, dựa trên các kết quả phân tích, điều tra, sử dụng các nguồn lực, phương tiện và nghiệp vụ của mình để tiến hành ngăn chặn các hành vi gây ra sự cố và hỗ trợ xử lý hậu quả;

h) Xác minh nguyên nhân và truy tìm nguồn gốc

Các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp sau khi phân tích sự cố, tham khảo các kết quả phân tích sự cố của các đơn vị khác, sử dụng các nguồn tin và quy trình nghiệp vụ của mình, chủ động điều tra chi tiết nguyên nhân và truy tìm nguồn gốc, gửi Cơ quan thường trực, Cơ quan điều phối quốc gia để tổng hợp, xác minh, báo cáo Ban Chỉ đạo quốc gia các thông tin liên quan, cụ thể bao gồm:

- Đối tượng bị tấn công;

- Phương thức thủ đoạn tấn công (quy trình, kỹ thuật, mẫu mã độc, phần mềm độc hại);

- Thời gian tấn công;

- Các thiệt hại đã xảy ra;

- Đối tượng tấn công;

- Dự đoán khả năng xảy ra các tấn công tương tự và thiệt hại.

6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia

Đơn vị chủ trì: Ban Chỉ đạo quốc gia

Nội dung thực hiện: Cơ quan thường trực tổng hợp toàn bộ các báo cáo phân tích có liên quan đến triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia để báo cáo với Ban Chỉ đạo quốc gia và họp phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung cho các sự cố tương tự.

7. Kết thúc

Đơn vị chủ trì: Cơ quan điều phối quốc gia

Đơn vị phối hợp: Chủ quản hệ thống thông tin, các đơn vị thuộc Bộ phận tác nghiệp ứng cứu khẩn cấp.

Nội dung thực hiện: Cơ quan điều phối quốc gia căn cứ kết quả đánh giá của Ban Chỉ đạo quốc gia sẽ thực hiện hoàn tất các nhiệm vụ sau, kết thúc hoạt động ứng cứu sự cố khẩn cấp:

- Lưu hồ sơ, tài liệu lưu trữ;

- Xây dựng, đúc rút các bài học, kinh nghiệm;

- Đề xuất các kiến nghị về kỹ thuật, chính sách để hạn chế thiệt hại khi xảy ra các tấn công tương tự;

- Báo cáo cơ quan cấp trên, tổ chức họp báo hoặc gửi thông tin cho truyền thông nếu cần thiết.

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

Điều 15. Trưng dụng tài sản và đình chỉ phương tiện thông tin phục vụ ứng cứu khẩn cấp sự cố an toàn thông tin mạng quốc gia

Trong quá trình triển khai ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia, khi được Cơ quan thường trực yêu cầu, các cơ quan có chức năng thẩm quyền theo quy định của pháp luật thực hiện:

1. Tạm đình chỉ hoặc đình chỉ việc sử dụng phương tiện thông tin liên lạc hoặc các hoạt động khác từ hệ thống thông tin khi có căn cứ xác định các hoạt động này gây nguy hại đặc biệt nghiêm trọng đến lợi ích công cộng hoặc tổn hại nghiêm trọng, đặc biệt nghiêm trọng tới quốc phòng, an ninh.

2. Trưng dụng phương tiện thông tin, phương tiện giao thông, phương tiện khác và người đang sử dụng, điều khiển phương tiện đó trong trường hợp cấp bách để thực hiện nhiệm vụ ứng cứu khẩn cấp hoặc để ngăn chặn hậu quả thiệt hại cho xã hội đang xảy ra hoặc có nguy cơ xảy ra.

3. Huy động các nguồn lực trong phạm vi ngành, lĩnh vực, địa phương mình quản lý để triển khai thực hiện ứng cứu sự cố.

Điều 16. Xây dựng và triển khai kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng

1. Các cơ quan, đơn vị xây dựng và thực hiện kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng (sau đây gọi tắt là kế hoạch ứng phó sự cố) để đảm bảo nhân lực, vật lực, tài 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, cụ thể như sau:

a) Cơ quan điều phối quốc gia xây dựng, trình Bộ Thông tin và Truyền thông phê duyệt để thực hiện kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng quốc gia và kế hoạch hoạt động của mạng lưới ứng cứu sự cố;

b) Đơn vị chuyên trách về ứng cứu sự cố của các bộ, cơ quan trung ương xây dựng, trình thủ trưởng cơ quan chủ quản phê duyệt để thực hiện kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng cho cơ quan nhà nước, tổ chức chính trị, tổ chức chính trị - xã hội trong phạm vi bộ, ngành mình quản lý;

c) Đơn vị chuyên trách về ứng cứu sự cố của các tỉnh, thành phố trực thuộc Trung ương xây dựng, trình Chủ tịch Ủy ban nhân dân cấp tỉnh phê duyệt để thực hiện kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng của địa phương;

d) Các thành viên mạng lưới, tổ chức, doanh nghiệp có quản lý hệ thống thông tin thuộc Danh mục hệ thống thông tin quan trọng quốc gia, hệ thống thông tin lớn, hệ thống điều khiển công nghiệp (SCADA) xây dựng, phê duyệt và thực hiện kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng trong tổ chức, doanh nghiệp mình.

2. Các cơ quan, đơn vị xây dựng kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng theo đề cương tại Phụ lục II của Quyết định này, trong đó chú trọng các nội dung: Các kịch bản tấn công, các nguy cơ, tình huống sự cố có khả năng xảy ra, các phương án ứng cứu theo các kịch bản, tình huống dự kiến và công tác huấn luyện, diễn tập. Trường hợp cần thiết, Bộ Thông tin và Truyền thông xem xét điều chỉnh một số điểm trong đề cương cho phù hợp với tình hình và yêu cầu sự cố an toàn thông tin mạng.

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; định kỳ kiểm tra, đánh giá việc triển khai kế hoạch ứng phó sự cố an toàn thông tin mạng của các bộ, ngành, địa phương và của các tổ chức, doanh nghiệp.

Điều 17. Kinh phí

1. Kinh phí để thực hiện các phương án, kế hoạch, hoạt động điều phối, ứng cứu, khắc phục sự cố an toàn thông tin mạng được lấy từ các nguồn: Ngân sách trung ương; ngân sách địa phương; kinh phí của doanh nghiệp và các nguồn vốn hợp pháp khác theo quy định.

2. Kinh phí thực hiện các hoạt động ứng cứu sự cố an toàn thông tin mạng được bố trí trong dự toán chi ngân sách nhà nước của các bộ, cơ quan trung ương và các địa phương (bao gồm chi đầu tư phát triển và chi thường xuyên) và được quản lý, sử dụng, thanh quyết toán theo phân cấp ngân sách quy định tại Luật ngân sách nhà nước và các văn bản hướng dẫn thi hành. Việc bố trí kinh phí thực hiện theo nguyên tắc: Hoạt động, lực lượng thuộc cơ quan cấp nào thì bố trí kinh phí và sử dụng từ nguồn kinh phí của cơ quan cấp đó, cụ thể:

a) Ngân sách trung ương bảo đảm cho:

- Hoạt động chỉ đạo, điều hành, kiểm tra, giám sát ứng cứu sự cố của Ban Chỉ đạo quốc gia, Ban Điều phối ứng cứu quốc gia, Cơ quan thường trực ứng cứu sự cố quốc gia;

- Hoạt động của Cơ quan điều phối quốc gia gồm: Kinh phí triển khai các hoạt động liên quan thuộc trách nhiệm của cơ quan điều phối quốc gia quy định tại các Điều 7, Điều 11, Điều 12, Điều 13, Điều 14 và Điều 16 Quyết định này; kinh phí bảo đảm hoạt động thường xuyên; tổ chức giám sát, phát hiện, cảnh báo; huấn luyện, diễn tập, đào tạo; mua sắm, nâng cấp, gia hạn bản quyền phần mềm, trang thiết bị, bảo dưỡng phương tiện, công cụ; tham gia, phối hợp các hoạt động hợp tác quốc tế về an toàn mạng; kinh phí xây dựng và triển khai kế hoạch ứng phó sự cố, kinh phí dự phòng ứng cứu, xử lý sự cố nghiêm trọng quốc gia; hỗ trợ các bộ, ngành, địa phương trong điều phối, ứng cứu sự cố; kinh phí thuê dịch vụ kỹ thuật, tổ chức và duy trì đội chuyên gia ứng cứu sự cố và bộ phận tác nghiệp ứng cứu sự cố; kinh phí điều hành và tổ chức các hoạt động của Mạng lưới ứng cứu sự cố, tuyên truyền, tập huấn, hội thảo, giao ban mạng lưới, nghiên cứu chuyên môn, duy trì bộ phận chuyên gia kỹ thuật, nâng cao năng lực và phát triển các đội ứng cứu sự cố; kinh phí kiểm tra, rà quét, đánh giá an toàn thông tin; tạo lập, thu thập, phân tích và chia sẻ thông tin về sự cố; hỗ trợ xây dựng, áp dụng chuẩn ISO 27xxx và các chuẩn quốc tế về an toàn thông tin mạng; triển khai các hoạt động nghiệp vụ đặc thù bảo đảm an toàn thông tin mạng cho các hệ thống thông tin quan trọng của Nhà nước;

- Các bộ, cơ quan trung ương căn cứ các nội dung quy định tại Quyết định này lập dự toán kinh phí hàng năm để triển khai các hoạt động liên quan thuộc trách nhiệm của bộ, ngành mình quy định tại các Điều 7, Điều 11, Điều 12, Điều 13, Điều 14 và Điều 16 Quyết định này; kinh phí xây dựng và triển khai kế hoạch ứng phó sự cố trong bộ, ngành mình; kinh phí dự phòng ứng cứu, xử lý sự cố cho các hệ thống thông tin do bộ, ngành mình quản lý; kinh phí tổ chức đào tạo, huấn luyện, diễn tập và hoạt động của Đội ứng cứu sự cố; 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 phạm vi quản lý.

b) Ngân sách địa phương bảo đảm cho hoạt động của Ban Chỉ đạo, đơn vị chuyên trách ứng cứu sự cố, đội ứng cứu sự cố của địa phương, gồm: Kinh phí để triển khai các hoạt động liên quan thuộc trách nhiệm của địa phương quy định tại các Điều 7, Điều 11, Điều 12, Điều 13, Điều 14 và Điều 16 Quyết định này; kinh phí triển khai kế hoạch ứng phó sự cố của địa phương; kinh phí dự phòng ứng cứu, xử lý sự cố cho các hệ thống thông tin thuộc địa phương quản lý; kinh phí tổ chức đào tạo, huấn luyện, diễn tập và hoạt động của Đội ứng cứu sự cố; 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 phạm vi quản lý;

c) Nguồn kinh phí của doanh nghiệp đảm bảo để triển khai các hoạt động liên quan thuộc trách nhiệm của doanh nghiệp quy định tại khoản 4 Điều 7, Điều 11, Điều 12, Điều 13, Điều 14 và Điều 16 Quyết định này; triển khai kế hoạch ứng

phó sự cố của doanh nghiệp, dự phòng ứng cứu, xử lý sự cố cho các hệ thống thông tin do doanh nghiệp quản lý; phối hợp giám sát, cung cấp thông tin, tham gia ứng cứu sự cố; tổ chức đào tạo, huấn luyện, diễn tập, duy trì hoạt động của Đội ứng cứu sự cố và các nhiệm vụ khác do doanh nghiệp thực hiện và được hạch toán vào chi phí kinh doanh để thực hiện. Các doanh nghiệp viễn thông, Internet bảo đảm kinh phí để giám sát, ứng cứu sự cố bảo đảm an toàn thông tin mạng trên các kênh kết nối Internet của doanh nghiệp mình và được hạch toán vào chi phí kinh doanh để thực hiện;

d) Chủ quản hệ thống thông tin phải bố trí kinh phí để thực hiện kế hoạch, phương án ứng cứu sự cố, dự phòng kinh phí xử lý sự cố, khắc phục hậu quả, khôi phục dữ liệu và hoạt động bình thường của hệ thống thông tin của mình;

đ) Nguồn vốn từ Quỹ dịch vụ viễn thông công ích Việt Nam được bố trí cho một số hoạt động, nhiệm vụ về điều phối, ứng cứu sự cố bảo đảm an toàn thông tin mạng mà ngân sách nhà nước không chi hoặc chi không đủ của cơ quan điều phối quốc gia, bộ phận tác nghiệp ứng cứu sự cố do cơ quan thường trực triệu tập, hoạt động của mạng lưới ứng cứu sự cố quốc gia, thuê dịch vụ kỹ thuật, tổ chức và duy trì đội chuyên gia ứng cứu sự cố thuộc cơ quan điều phối quốc gia, chi trả cho hao tổn của các doanh nghiệp viễn thông, Internet do triển khai giải pháp ứng cứu, ngăn chặn, xử lý sự cố nghiêm trọng quốc gia, và các hoạt động khác liên quan mà ngân sách nhà nước không chi hoặc chi không đủ;

e) Bộ Tài chính chủ trì, phối hợp với Bộ Thông tin và Truyền thông hướng dẫn chi tiết kinh phí cho công tác điều phối, ứng cứu sự cố bảo đảm an toàn thông tin mạng quy định tại Điều này.

Chương V
ĐIỀU KHOẢN THI HÀNH

Điều 18. Hiệu lực thi hành

Quyết định này có hiệu lực thi hành kể từ ngày ký ban hành.

Điều 19. Tổ chức thực hiện

Bộ, cơ quan ngang Bộ, cơ quan trung ương, Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương và các tổ chức liên quan triển khai thực hiện Quyết định này.

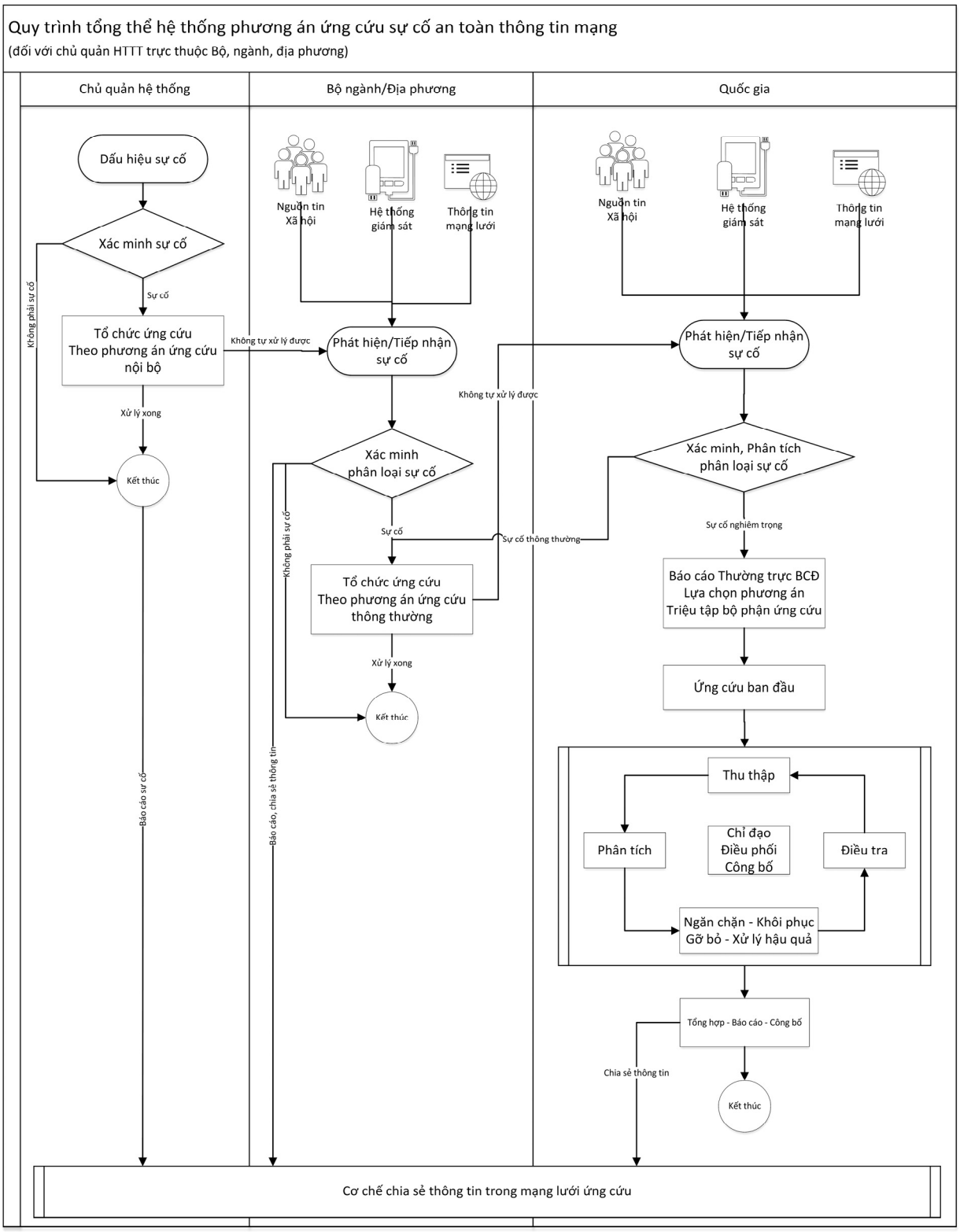
Trong quá trình thực hiện nếu phát sinh vướng mắc hoặc nhận thấy cần thiết phải thay đổi những nội dung quy định trong Quyết định này, các cơ quan, tổ chức có ý kiến bằng văn bản gửi Bộ Thông tin và Truyền thông tổng hợp, báo cáo Thủ tướng Chính phủ để xem xét sửa đổi, bổ sung./.

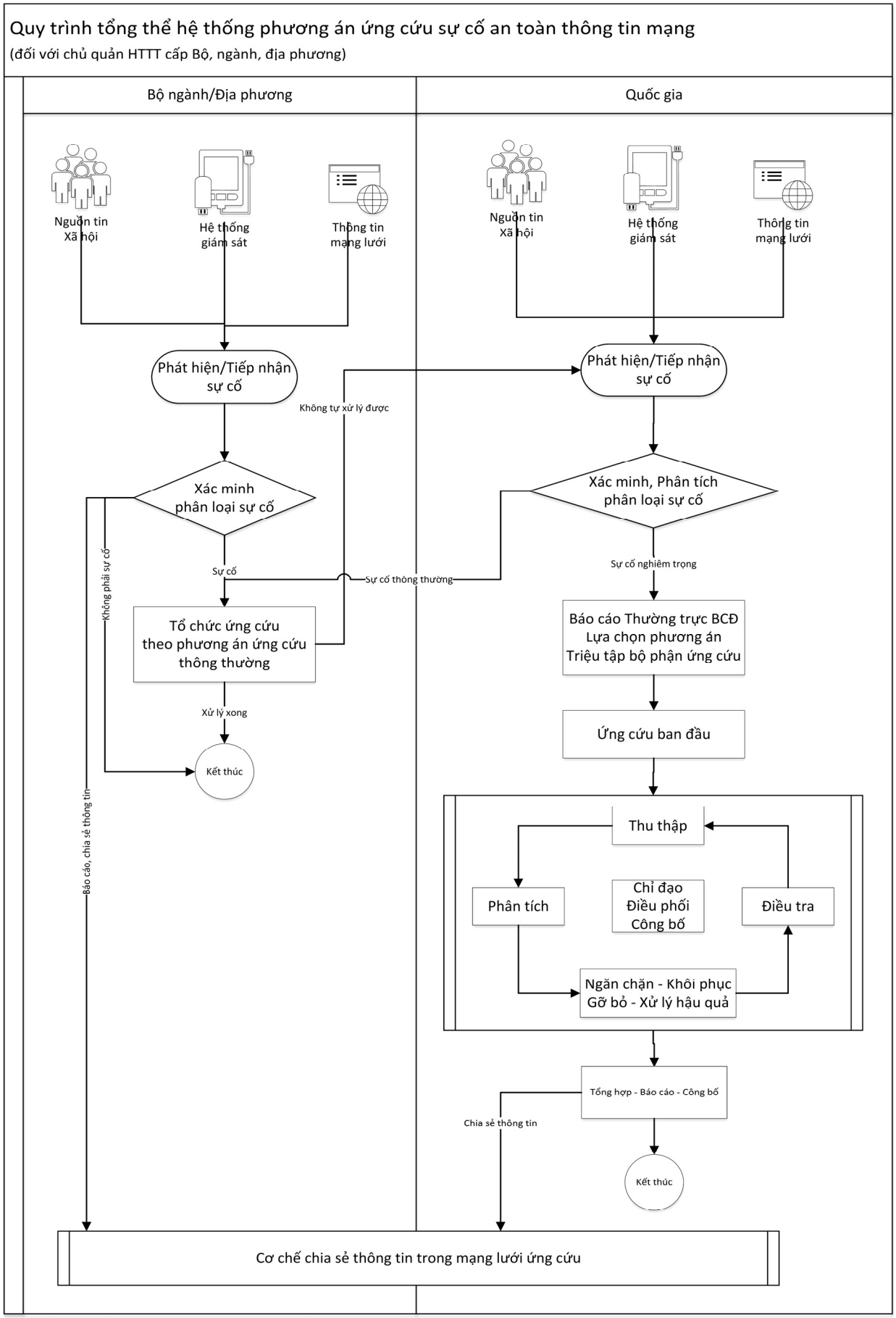
THỦ TƯỚNG

Nguyễn Xuân Phúc

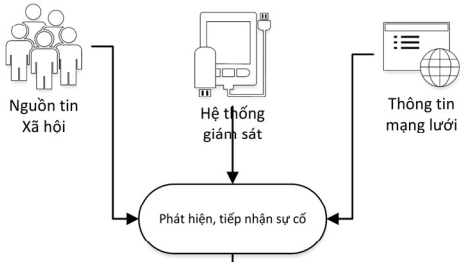
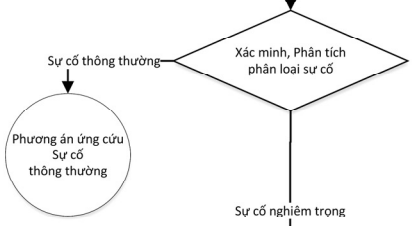
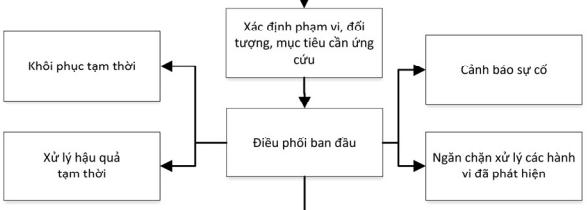
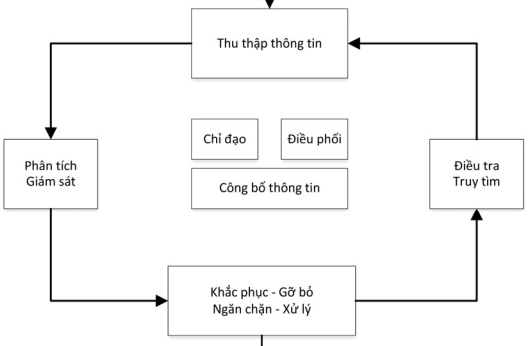
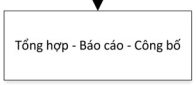
Phụ lục I
QUY TRÌNH ĐIỀU PHỐI, ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG

(Kèm theo Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ)




Quy trình tổng thể hệ thống phương án ứng cứu sự cố an toàn thông tin mạng
(đối với chủ quản HTTT cấp Bộ, ngành, địa phương)
Bộ ngành/Địa phương
Quốc gia
Nguồn tin Xã hội
Hệ thống giám sát
Thông tin mạng lưới
Nguồn tin Xã hội
Hệ thống giám sát
Thông tin mạng lưới
Phát hiện/Tiếp nhận sự cố
Phát hiện/Tiếp nhận sự cố
Không tự xử lý được
Xác minh phân loại sự cố
Xác minh, Phân tích phân loại sự cố
Không phải sự cố
Sự cố
Sự cố thông thường
Sự cố nghiêm trọng
Tổ chức ứng cứu theo phương án ứng cứu thông thường
Báo cáo Thường trực BCĐ Lựa chọn phương án Triệu tập bộ phận ứng cứu
Xử lý xong
Ứng cứu ban đầu
Kết thúc
Báo cáo, chia sẻ thông tin
Thu thập
Phân tích
Chỉ đạo Điều phối Công bố
Điều tra
Ngăn chặn - Khôi phục Gỡ bỏ - Xử lý hậu quả
Tổng hợp - Báo cáo - Công bố
Chia sẻ thông tin
Kết thúc
Cơ chế chia sẻ thông tin trong mạng lưới ứng cứu

Quy trình ứng cứu khẩn cấp sự cố quan trọng

	Thành phần	Quy trình	Ghi chú
Bước 1	- Cơ quan điều phối quốc gia		- Chủ quản HTTT - Các nguồn tin xã hội - Các hệ thống giám sát - Thông tin mạng lưới
Bước 2	- Cơ quan điều phối quốc gia - Chủ quản hệ thống thông tin		- VNCERT phối hợp cùng chủ quản hệ thống thông tin xác minh và phân loại sự cố. - Nếu là sự cố thông thường các đơn vị sẽ tiến hành theo Phương án ứng cứu xây dựng sẵn. - Nếu là sự cố nghiêm trọng, tiến hành bước tiếp theo.
Bước 3	- Cơ quan thường trực - Thành phần tham gia Bộ phận ứng cứu		- VNCERT báo cáo Cơ quan thường trực. - BCĐ QG chấp nhận phương án phân loại sự cố. - BCĐ QG triệu tập bộ phân ứng cứu
Bước 4	- Cơ quan điều phối quốc gia - Thành phần tham gia Bộ phận ứng cứu		
Bước 5	- Cơ quan thường trực - Ban điều phối quốc gia - Cơ quan điều phối quốc gia - Thành phần tham gia Bộ phận ứng cứu		- Các thành phần tham gia bộ phận ứng cứu triển khai ngay các công đoạn ứng cứu với nguồn lực và quy trình nghiệp vụ của mình, đồng thời tuân thủ cơ chế phối hợp và chia sẻ thông tin. - Các công đoạn này được triển khai liên tục, lặp lại tùy thuộc vào diễn biến của sự cố. - Ban điều phối quốc gia đóng vai trò điều phối, giám sát cơ chế phối hợp và chia sẻ thông tin.
Bước 6	- Ban chỉ đạo - Cơ quan thường trực - Cơ quan điều phối quốc gia - Thành phần tham gia Bộ phận ứng cứu		

Phụ lục II

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

(Kèm theo Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ)

1. Các quy định chung

a) Phạm vi và đối tượng của kế hoạch;

b) Nguyên tắc, 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 quản lý, 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 bảo đảm an toàn thông tin mạng;
- Bộ phận tác nghiệp ứng cứu khẩn cấp;
- Cơ quan điều phối quốc gia;
- Ban Chỉ đạo ứng cứu khẩn cấp sự cố;
- Cơ quan thường trực và Ban Chỉ đạo quốc gia;
- 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 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.

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 11, Điều 12, Điều 13, Điều 14 và các nội dung liên quan khác của Quyết định 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 3 Phụ lục này;

- 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 tác nghiệp 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./