

TH (2)

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

SNG THÔNG TIN ĐIỆN TỬ CHÍNH PHỦ	
ĐẾN	Giới: C
	Ngày: 20.13.117

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.