

Số: **2711**/QĐ-UBND

Thừa Thiên Huế, ngày **17** tháng **11** năm 2017

QUYẾT ĐỊNH

Ban hành Quy chế phối hợp giữa các cơ quan, đơn vị trong việc ứng phó sự cố máy tính, đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Thừa Thiên Huế

CÔNG THÔNG TIN ĐIỆN TỬ T.T.HUẾ	
ĐỀ	Số: 1496
	Ngày: 22/11
	Chuyên: Căn cứ Luật

ỦY BAN NHÂN DÂN TỈNH

Tô chức Chính quyền địa phương ngày 19 tháng 6 năm 2015;

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

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

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ Thông tin và Truyền thông về việc Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế phối hợp giữa các cơ quan, đơn vị trong việc ứng phó sự cố máy tính, đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Thừa Thiên Huế.

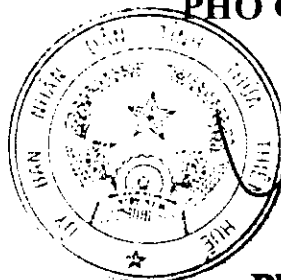
Điều 2. Quyết định này có hiệu lực kể từ ngày ký.

Điều 3. Chánh Văn phòng Ủy ban nhân dân tỉnh; Giám đốc: Sở Thông tin và Truyền thông, Giám đốc Công an tỉnh, Chỉ huy trưởng Bộ Chỉ huy Quân sự tỉnh, Thủ trưởng các sở, ban ngành cấp tỉnh; Chủ tịch Ủy ban nhân dân các huyện, thị xã, thành phố Huế; Các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:

- Như Điều 3;
- Bộ Thông tin và Truyền thông (b/c);
- TVTU, TT HĐND (b/c);
- CT, các PCT UBND tỉnh;
- Các doanh nghiệp CNTT, Viễn thông;
- Công Thông tin điện tử tỉnh;
- VP: CVP và các PCVP UBND tỉnh;
- Lưu: VT, CT.

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



Phan Ngọc Thọ

QUY CHẾ

Phối hợp giữa các cơ quan, đơn vị trong việc ứng phó sự cố máy tính, đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Thừa Thiên Huế
*(ban hành kèm theo Quyết định số **2711** /QĐ-UBND ngày **17/11/2017** của UBND tỉnh Thừa Thiên Huế)*

CHƯƠNG I

CÁC QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh

Quy chế này quy định đối tượng, mục tiêu, nguyên tắc, nội dung và trách nhiệm phối hợp giữa các cơ quan, đơn vị; cơ quan địa phương – cơ quan trung ương trong việc nâng cao năng lực phòng chống phần mềm độc hại, ứng phó sự cố máy tính, đảm bảo an toàn thông tin mạng, cải thiện độ tin cậy của quốc gia trong hoạt động giao dịch điện tử theo hướng xã hội hóa.

Điều 2. Đối tượng áp dụng

1. Các Sở, ban, ngành cấp tỉnh; UBND các huyện, thị xã, thành phố; Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và các đơn vị, cá nhân trực tiếp tham gia hoặc có liên quan đến hoạt động phòng chống phần mềm độc hại, ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng.

2. Các doanh nghiệp cung cấp dịch vụ viễn thông, công nghệ thông tin (CNTT), Internet; các cơ quan, đơn vị liên quan.

Điều 3. Mục đích phối hợp

1. Thiết lập cơ chế phối hợp đồng bộ, chặt chẽ giữa các cơ quan, đơn vị; địa phương – trung ương trong hoạt động ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng trên địa bàn tỉnh, cũng như quốc gia; sẵn sàng, chủ động phòng ngừa và xử lý các tình huống phát sinh trong lĩnh vực ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng; bảo đảm an toàn các hệ thống thông tin trọng yếu; sẵn sàng đối phó với các cuộc tấn công mạng.

2. Nâng cao trách nhiệm phối hợp giữa các cơ quan, đơn vị; giữa địa phương – trung ương, đảm bảo công tác phối hợp xử lý, khắc phục sự cố về máy tính, an toàn thông tin mạng được kịp thời, nhanh chóng.

3. Đảm bảo cơ sở hạ tầng, hệ thống mạng, thiết bị viễn thông, công nghệ thông tin, các hệ thống thông tin dùng chung của tỉnh, của quốc gia, cổng/trang

thông tin điện tử,... hoạt động an toàn, bảo mật nhằm đẩy mạnh ứng dụng công nghệ thông tin trong hoạt động của cơ quan Nhà nước, phục vụ tốt công tác chỉ đạo, điều hành.

Điều 4. Nguyên tắc phối hợp

1. Đảm bảo thống nhất, đồng bộ, hiệu quả, phân công rõ trách nhiệm của từng cơ quan trong việc chủ trì, phối hợp thực hiện trong hoạt động ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng.

2. Việc thực hiện các nhiệm vụ phối hợp phải trên cơ sở chức năng, nhiệm vụ, quyền hạn được giao; tuân thủ các quy định của Quy chế này và các quy định của pháp luật có liên quan.

3. Đảm bảo bí mật quốc gia, bảo mật thông tin theo quy định của pháp luật; bảo đảm hệ thống mạng, thiết bị viễn thông, công nghệ thông tin hoạt động liên tục và an toàn.

4. Thông tin được trao đổi, cung cấp trong quá trình phối hợp được bảo đảm bí mật theo yêu cầu của tổ chức, cá nhân tham gia phối hợp.

5. Quá trình phối hợp không làm cản trở hoạt động bình thường và tổn hại đến quyền, lợi ích hợp pháp của các tổ chức, cá nhân có liên quan.

6. Chịu trách nhiệm về nội dung, kết quả phối hợp.

7. Tùy theo tính chất, mức độ và nội dung công việc cần phối hợp, cơ quan chủ trì xem xét mời thêm các đơn vị có liên quan để hỗ trợ giải quyết công việc nhanh chóng, thuận lợi.

CHƯƠNG II

NỘI DUNG VÀ TRÁCH NHIỆM PHỐI HỢP

Điều 5. Phối hợp tuyên truyền, phổ biến nâng cao nhận thức và trách nhiệm về ứng phó sự cố máy tính, đảm bảo an toàn thông tin mạng

1. Trách nhiệm của Sở Thông tin và Truyền thông:

a) Tổ chức phổ biến Quy chế phối hợp giữa các cơ quan, đơn vị trong việc ứng phó sự cố máy tính, đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Thừa Thiên Huế ban hành kèm theo Quyết định này. Xây dựng Kế hoạch triển khai thực hiện Đề án Tuyên truyền, phổ biến, nâng cao nhận thức và trách nhiệm về ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng tại Quyết định số 05/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ.

b) Phối hợp với các cơ quan báo chí xây dựng nội dung tuyên truyền, phổ biến về ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng.

c) Hướng dẫn các đơn vị chức năng, các phòng Văn hóa và Thông tin các huyện, thị xã, thành phố triển khai thực hiện nghiêm túc các quy định về ứng phó sự cố máy tính, đảm bảo an toàn thông tin mạng.

d) Chủ trì xây dựng bản tin hàng quý về ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng phục vụ công tác lãnh đạo, chỉ đạo gửi các cấp ủy Đảng, cơ quan trong tỉnh.

2. Trách nhiệm của Công an tỉnh:

a) Phối hợp với Sở Thông tin và Truyền thông tuyên truyền nâng cao nhận thức về ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng; tăng cường công tác giáo dục chính trị, tư tưởng, bảo vệ chính trị nội bộ, bảo vệ Đảng, bảo vệ chế độ và bảo vệ bí mật Nhà nước; tuyên truyền, làm rõ các hình thức, thủ đoạn lợi dụng mạng Internet của các thế lực thù địch để hoạt động chống phá Nhà nước, xâm phạm an ninh quốc gia nhằm nâng cao ý thức cảnh giác cho cán bộ, công chức, viên chức trong việc truy cập, khai thác thông tin trên Internet, sử dụng các mạng xã hội; tuyên truyền, phổ biến pháp luật về xử lý tội phạm trong lĩnh vực công nghệ thông tin.

b) Cung cấp tin, bài viết thuộc lĩnh vực an ninh thông tin đối với bản tin hàng quý về an toàn, an ninh thông tin.

c) Khi có đề nghị bằng văn bản hoặc đề nghị trực tiếp của Sở Thông tin và Truyền thông, Công an tỉnh kịp thời phối hợp thực hiện các nội dung tuyên truyền, phổ biến nâng cao nhận thức về an toàn, an ninh thông tin mạng theo trách nhiệm của mình.

d) Phối hợp cung cấp cho Sở Thông tin và Truyền thông các thông tin mới nhất liên quan đến lĩnh vực bảo đảm an ninh thông tin (nếu có thể).

3. Trách nhiệm của các cơ quan trung ương đóng trên địa bàn:

a) 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 phó sự cố máy tính đảm bảo an toàn thông tin mạng.

b) Xây dựng, triển khai và vận hành công 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.

Điều 6. Phối hợp trong đảm bảo cơ sở hạ tầng, hệ thống mạng, thiết bị viễn thông, công nghệ thông tin, các hệ thống thông tin dùng chung của tỉnh

1. Trách nhiệm của Sở Thông tin và Truyền thông:

a) Đề xuất UBND tỉnh các giải pháp phòng ngừa và ngăn chặn các hành vi vi phạm về an toàn thông tin theo hướng dẫn, yêu cầu của cơ quan cấp trên.

b) Kiểm tra các điểm yếu, lỗ hổng bảo mật trên các hệ thống thông tin quan trọng, trọng yếu, các phần mềm ứng dụng dùng chung của tỉnh như: Cổng thông tin điện tử, Hệ thống Hội nghị Truyền hình, Hệ thống thư điện tử công vụ...

c) Triển khai các giải pháp kỹ thuật bảo đảm các hệ thống thông tin quan trọng được an toàn, bảo mật, đặc biệt là tại Trung tâm Thông tin dữ liệu điện tử tỉnh bảo đảm hoạt động liên tục và an toàn.

d) Phối hợp với Công an tỉnh triển khai các sản phẩm bảo mật mạng công nghệ thông tin đối với các ứng dụng công nghệ thông tin, hệ thống thông tin quan trọng; triển khai các hệ thống giám sát an toàn thông tin đối với các mạng CNTT trọng yếu: mạng tin học diện rộng của tỉnh, Trung tâm Thông tin dữ liệu điện tử tỉnh, hệ thống Hội nghị truyền hình tỉnh, nhằm sớm phát hiện các nguy cơ, kịp thời phát hiện sự cố và dấu hiệu tấn công, đảm bảo an toàn cho các hệ thống thông tin dùng chung, các hệ thống đang cài đặt vận hành, hosting tại Trung tâm Thông tin dữ liệu điện tử tỉnh.

2. Trách nhiệm của Công an tỉnh:

a) Kiểm soát, phòng ngừa, đấu tranh, ngăn chặn các loại tội phạm mạng lợi dụng hệ thống thông tin gây mất an ninh thông tin mạng trên địa bàn tỉnh.

b) Điều tra, ngăn chặn và xử lý các hành vi vi phạm pháp luật về an ninh thông tin mạng; các hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội trên địa bàn tỉnh.

c) Trao đổi, cung cấp Sở Thông tin và Truyền thông về âm mưu, phương thức hoạt động của các thế lực thù địch, tội phạm công nghệ cao nhằm mục đích chống Đảng, Nhà nước để phối hợp có biện pháp phòng ngừa, phát hiện và ngăn chặn kịp thời.

d) Kiểm định các thiết bị viễn thông, công nghệ thông tin theo quy định trước khi đưa vào sử dụng tại các bộ phận trọng yếu, cơ mật.

đ) Thực hiện nhiệm vụ bảo vệ an toàn các công trình quan trọng về an ninh quốc gia trên lĩnh vực bưu chính, viễn thông và công nghệ thông tin.

e) Triển khai các biện pháp nghiệp vụ, kiểm soát thông tin chuyên qua mạng theo quy định của pháp luật nhằm phát hiện, ngăn chặn, xử lý kịp thời các hành vi vi phạm.

g) Chỉ đạo Công an các huyện, thị xã, thành phố triển khai công tác bảo đảm an ninh thông tin, phòng chống tội phạm; phối hợp chặt chẽ với Sở Thông tin và Truyền thông để đảm bảo an ninh cơ sở hạ tầng mạng.

h) Đề xuất với Bộ Công an hỗ trợ kinh phí đầu tư, trang bị phương tiện kỹ thuật cho Công an tỉnh để nâng cao năng lực bảo đảm an ninh thông tin mạng, đủ khả năng phòng ngừa, phát hiện, ngăn chặn hoạt động của các thế lực thù địch, phản động và tội phạm mạng.

i) Phối hợp Sở Thông tin và Truyền thông trong việc đề xuất UBND tỉnh các giải pháp phòng ngừa và ngăn chặn các hành vi vi phạm theo hướng dẫn, yêu cầu của cơ quan cấp trên.

k) Tham gia tư vấn yêu cầu kỹ thuật liên quan đến công tác đầu tư hệ thống đảm bảo an ninh thông tin của Sở Thông tin và Truyền thông.

l) Triển khai các giải pháp đấu tranh có hiệu quả với hoạt động của các thế lực thù địch, phản động, tội phạm mạng lợi dụng dịch vụ viễn thông, Internet để xâm phạm an ninh, trật tự an toàn xã hội; phát hiện, xử lý kịp thời các hành vi vi phạm an ninh thông tin.

3. Trách nhiệm của Bộ Chỉ huy Quân sự tỉnh:

a) Bồi dưỡng lực lượng tác chiến mạng của Bộ Chỉ huy Quân sự tỉnh có tính chiến đấu cao, tham gia giám sát, bảo vệ hạ tầng mạng trọng yếu của tỉnh và thực hiện nhiệm vụ bảo vệ chủ quyền quốc gia trên không gian mạng.

b) Triển khai các giải pháp, biện pháp đề phòng ngừa, đấu tranh, ngăn chặn, làm thất bại các âm mưu tuyên truyền phản động, phá hoại nội bộ, kích động quần chúng biểu tình trái pháp luật, hoạt động khủng bố, chống chính quyền; các hoạt động tấn công thâm nhập hệ thống mạng quốc gia.

c) Đấu tranh, ngăn chặn các thế lực thù địch, phản động xâm nhập hệ thống mạng quốc gia.

d) Tiến hành các hoạt động nghiệp vụ quốc phòng, an ninh khác đảm bảo theo chức năng, nhiệm vụ và quyền hạn được giao.

đ) Đề xuất tăng cường đầu tư trang bị phương tiện đặc thù nhằm bảo vệ chủ quyền không gian mạng; Đề xuất với Bộ Quốc phòng hỗ trợ kinh phí đầu tư, trang bị phương tiện kỹ thuật nhằm bảo vệ chủ quyền không gian mạng.

4. Trách nhiệm của các doanh nghiệp cung cấp dịch vụ viễn thông, CNTT và Internet:

a) 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 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 các cơ quan, đơn vị.

b) Đầu tư xây dựng, trang bị hạ tầng kỹ thuật đáp ứng đầy đủ các yêu cầu, tiêu chuẩn kỹ thuật theo quy định của Bộ Thông tin và Truyền thông về an ninh mạng và an toàn thông tin và các nội dung quy định tại Quy chế này.

5. Trách nhiệm của các cơ quan, đơn vị:

a) Quan tâm, chú trọng đến công tác bảo đảm ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng cho hệ thống thông tin tại đơn vị mình.

b) Chủ động bố trí kinh phí trang bị phần mềm chống virus, thiết bị tường lửa cho hệ thống máy tính, hệ thống mạng, hệ thống thông tin tại đơn vị mình.

c) Phối hợp với Sở Thông tin và Truyền thông và các đơn vị liên quan thực hiện công tác ứng phó sự cố máy tính, an toàn thông tin mạng trên địa bàn tỉnh.

Điều 7. Phối hợp xử lý, khắc phục về sự cố máy tính, an toàn thông tin mạng

1. Trách nhiệm của Sở Thông tin và Truyền thông:

a) Thành lập bộ phận đầu mối tiếp nhận thông tin về sự cố mạng và hỗ trợ các tổ chức, cá nhân xử lý và khắc phục sự cố trong khả năng và trách nhiệm của mình.

b) Tùy theo tính chất, nội dung công việc cần phối hợp với các cơ quan khác, Sở Thông tin và Truyền thông phát hành văn bản hoặc thư điện tử, điện thoại, fax đề nghị Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và các cơ quan có liên quan phối hợp tham gia xử lý, khắc phục ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng theo chức năng, nhiệm vụ và quyền hạn được giao.

c) Trong trường hợp sự cố không thể khắc phục được, Sở Thông tin và Truyền thông đề nghị Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh huy động các nguồn lực khác, mời chuyên gia tham gia xử lý, khắc phục sự cố.

d) Thông báo sự cố về Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) hoặc cơ quan khác trong trường hợp không xử lý, khắc phục sự cố được.

đ) Đề nghị cơ quan có thẩm quyền xử lý các tổ chức, cá nhân vi phạm về an toàn, an ninh thông tin mạng theo quy định.

e) Đối với những vi phạm có liên quan đến sự cố máy tính, an toàn thông tin mạng phải thông báo ngay cho Công an tỉnh để điều tra xác minh, xử lý theo pháp luật.

g) Phối hợp với Công an tỉnh thu thập, chuyên tài liệu, chứng cứ của các đối tượng lợi dụng mạng để hoạt động phạm tội (khi có yêu cầu của cơ quan Công an).

2. Trách nhiệm của Công an tỉnh:

a) Cử cán bộ có chuyên môn, nghiệp vụ phụ trách theo dõi, làm đầu mối phối hợp trong hoạt động bảo đảm ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng và phối hợp thực hiện xử lý, khắc phục sự cố theo chức năng, nhiệm vụ và quyền hạn được giao.

b) Khi phát hiện những dấu hiệu, các hành vi vi phạm pháp luật trong hoạt động đảm ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng, thông báo cho Sở Thông tin và Truyền thông, Bộ Chỉ huy Quân sự tỉnh để phối hợp xử lý.

c) Điều tra và xử lý các trường hợp vi phạm pháp luật về ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng theo quy định của pháp luật; áp dụng các biện pháp nghiệp vụ ngăn chặn, xử lý ngay các hành vi gây ảnh hưởng nghiêm trọng đến các hệ thống thông tin trọng yếu của tỉnh.

d) Hỗ trợ về nhân lực, phần mềm, thiết bị chuyên dùng theo khả năng khi có đề nghị của Sở Thông tin và Truyền thông để điều tra làm rõ các hành vi tấn công mạng.

3. Trách nhiệm của Bộ Chỉ huy Quân sự tỉnh:

a) Thông báo đến Sở Thông tin và Truyền thông, Công an tỉnh khi phát hiện những dấu hiệu, các hành vi gây phương hại đến quốc phòng, an ninh để phối hợp xử lý.

b) Cử cán bộ có trình độ, năng lực phụ trách việc theo dõi các hành vi gây phương hại đến quốc phòng, an ninh trên không gian mạng và phối hợp xử lý, khắc phục sự cố theo chức năng, nhiệm vụ và quyền hạn được giao.

c) Hỗ trợ về nhân lực, thiết bị chuyên dụng để điều tra, xử lý, khắc phục sự cố khi có yêu cầu của Sở Thông tin và Truyền thông.

d) Xử lý các tổ chức, cá nhân chủ mưu thực hiện hành vi gây phương hại đến quốc phòng - an ninh theo quy định của pháp luật.

4. Trách nhiệm của các cơ quan trung ương đóng trên địa bàn

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.

Điều 8. Phối hợp đào tạo, bồi dưỡng kiến thức về ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng

1. Trách nhiệm của Sở Thông tin và Truyền thông:

Xây dựng kế hoạch, tổ chức đào tạo, bồi dưỡng kiến thức, kỹ năng về ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng cho cán bộ, công chức, viên chức trong các cơ quan hành chính nhà nước trên địa bàn tỉnh.

2. Trách nhiệm của Công an tỉnh:

a) Phối hợp với Sở Thông tin và Truyền thông mời các đơn vị nghiệp vụ thuộc Bộ Công an để đào tạo, bồi dưỡng kiến thức, kỹ năng về ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng cho cán bộ, công chức, viên chức trong các cơ quan hành chính nhà nước trên địa bàn tỉnh.

b) Phối hợp Sở Thông tin và Truyền thông tổ chức các lớp tập huấn, bồi dưỡng kiến thức pháp luật về công tác bảo vệ bí mật nhà nước trong lĩnh vực thông tin và truyền thông; công tác phòng chống các loại tội phạm lợi dụng hoạt động thông tin và truyền thông xâm phạm an ninh quốc gia và trật tự an toàn xã hội cho cán bộ các cấp, các tổ chức và cá nhân có liên quan.

3. Trách nhiệm của các cơ quan trung ương đóng trên địa bàn

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.

Điều 9. Phối hợp kiểm tra, đánh giá thực trạng ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng

1. Trách nhiệm của Sở Thông tin và Truyền thông:

a) Định kỳ hàng năm, xây dựng kế hoạch, tổ chức kiểm tra, đánh giá công tác đảm bảo ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh và thông báo cho Công an tỉnh để phối hợp.

b) Cung cấp các văn bản, tài liệu có liên quan... cho Công an tỉnh (nếu có) để nghiên cứu, kiểm tra, đánh giá.

c) Xây dựng và diễn tập về ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng thuộc phạm vi của tỉnh với các phương án, kịch bản phù hợp thực tế.

2. Trách nhiệm của Công an tỉnh:

a) Cử cán bộ tham gia đoàn kiểm tra, đánh giá công tác đảm bảo ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh.

b) Định kỳ, tổ chức kiểm tra việc triển khai bảo đảm ứng phó sự cố máy tính đảm bảo an toàn thông tin mạng trong hoạt động Internet của các chủ thể cung cấp dịch vụ.

c) Phối hợp đánh giá thực trạng hệ thống an toàn, bảo mật thông tin tại Trung tâm Thông tin dữ liệu điện tinh, hệ thống phát hiện, cảnh báo các dấu hiệu bất thường liên quan đến công tác bảo mật.

d) Thanh tra, kiểm tra và xử lý vi phạm về sự cố máy tính, an toàn thông tin mạng trong hoạt động ứng dụng và phát triển công nghệ thông tin.

CHƯƠNG III TỔ CHỨC THỰC HIỆN

Điều 10. Trách nhiệm thi hành

1. Giám đốc Sở Thông tin và Truyền thông, Giám đốc Công an tỉnh, Chỉ huy trưởng Bộ Chỉ huy Quân sự tỉnh và các đơn vị có liên quan có trách nhiệm tổ chức triển khai thực hiện nghiêm túc Quy chế này.

2. Giám đốc Sở Thông tin và Truyền thông chủ trì, phối hợp với Giám đốc Công an tỉnh, Chỉ huy trưởng Bộ Chỉ huy Quân sự tỉnh giúp Chủ tịch Ủy ban nhân dân tỉnh phổ biến, triển khai, theo dõi, đôn đốc, kiểm tra việc thực hiện Quy chế này; báo cáo Chủ tịch Ủy ban nhân dân tỉnh kết quả thực hiện.

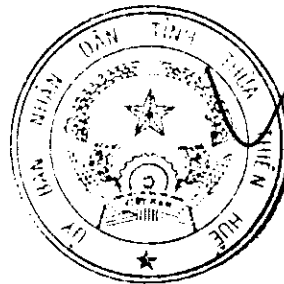
Điều 11. Khen thưởng, xử lý trách nhiệm

1. Sở Thông tin và Truyền thông, Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh định kỳ tổ chức sơ kết, đánh giá việc thực hiện Quy chế này; xét khen thưởng các đơn vị, cá nhân có thành tích tiêu biểu trong thực hiện Quy chế.

2. Cơ quan, đơn vị, cá nhân vi phạm Quy chế này bị xử lý trách nhiệm theo quy định của pháp luật.

Trong quá trình thực hiện Quy chế này nếu có vấn đề vướng mắc, phát sinh, các cơ quan, đơn vị phản ánh kịp thời về Sở Thông tin và Truyền thông để tổng hợp báo cáo Ủy ban nhân dân tỉnh điều chỉnh, bổ sung./.

**TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Phan Ngọc Thọ