ỦY BAN NHÂN DÂN
THÀNH PHỐ HỒ CHÍ MINH
ĐỘI ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG THÀNH PHỐ

Số : 207 /QĐ-STTTT

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

Thành phố Hồ Chí Minh, ngày 02 tháng 7 năm 2020

QUYẾT ĐỊNH

Về ban hành Quy định hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hồ Chí Minh

ĐỘI TRƯỞNG ĐỘI ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG THÀNH PHỐ

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

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 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 Quyết định số 1622/QĐ-TTg ngày 25 tháng 10 năm 2017 của Thủ tướng Chính phủ về phê duyệt Đề án đẩy mạnh hoạt động của mạng lưới ứng cứu sự cố, tăng cường năng lực cho các cán bộ, bộ phận chuyên trách ứng cứu sự cố an toàn thông tin mạng trên toàn quốc đến 2020, định hướng đến 2025;

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ Thông tin và Truyền thông về Quy định chi tiết và hướng dẫn một số điều của 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 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông Quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc;

Căn cứ Quyết định số 777/QĐ-UBND ngày 06 tháng 3 năm 2020 của Ủy ban nhân dân thành phố Hồ Chí Minh về việc thành lập Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hồ Chí Minh;

Xét đề nghị của Phòng Công nghệ thông tin tại Phiếu trình số 355/TT-CNTT ngày 21 tháng 7 năm 2020 về Quy định hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hồ Chí Minh,

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy định về hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hồ Chí Minh".

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

Điều 3. Văn phòng Ủy ban nhân dân thành phố, Sở Nội vụ, Sở Thông tin và Truyền thông, Sở Tài chính, Công an thành phố, Bộ Tư lệnh thành phố, Ủy ban nhân dân các quận, huyện, các cá nhân và đơn vị có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Chi hội An toàn thông tin phía Nam;
- Trung tâm An ninh mạng;
- Cty TNHH MTV QTSC;
- Ban Giám đốc Sở TTTT;
- Trung tâm CNTTTT;
- Lưu: VT, CNTT (LP.39).

ĐỘI TRƯỞNG

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
THÀNH PHỐ HỒ CHÍ MINH

PHÓ GIÁM ĐỐC SỞ THÔNG TIN VÀ TRUYỀN THÔNG
Võ Thị Trung Trinh

QUY ĐỊNH
Về hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng Thành phố Hồ Chí Minh

(Ban hành kèm theo Quyết định số 207/QĐ-STTTT ngày 02 tháng 7 năm 2020)

Chương I
NHỮNG QUY ĐỊNH CHUNG

Điều 1. Phạm vi điều chỉnh và đối tượng áp dụng

Quy định này điều chỉnh trách nhiệm, quyền hạn, chế độ làm việc, nguyên tắc hoạt động, nguyên tắc điều phối ứng cứu sự cố và các điều kiện cần thiết để duy trì hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hồ Chí Minh (sau đây viết tắt là Đội ứng cứu).

Đối tượng áp dụng là các cá nhân, tổ chức được nêu tại Quyết định số 777/QĐ-UBND ngày 06/3/2020 của Ủy ban nhân dân thành phố về việc thành lập Đội ứng cứu sự cố an toàn thông tin mạng thành phố Hồ Chí Minh và các cá nhân, tổ chức có liên quan đến hoạt động điều phối, ứng cứu sự cố mạng, máy tính trên địa bàn thành phố.

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 ATTTM).

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, cá nhân hoặc đơn vị có liên quan được quy định tại Quyết định số 777/QĐ-UBND ngày 06/3/2020 của Ủy ban nhân dân thành phố.

Điều 3. Chức năng và nhiệm vụ của Đội ứng cứu

1. 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.

2. Phối hợp các đơn vị, cơ quan liên quan 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 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông, tham mưu giúp Sở Thông tin và Truyền thông trình Ủy ban nhân dân thành phố và Cơ quan điều phối quốc gia về ATANM.

3. Tham mưu giúp Sở Thông tin và Truyền thông báo cáo với Ủy ban nhân dân thành phố khi tiếp nhận thông tin, phát hiện các sự cố đối với hệ thống thông tin trong phạm vi quản lý.

4. Tham mưu giúp Sở Thông tin và Truyền thông 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 các đơn vị có liên quan quy định

tại Điều 7 Quyết định số 777/QĐ-UBND ngày 06/3/2020 của Ủy ban nhân dân thành phố Hồ Chí Minh.

5. Có quyền đề nghị các thành viên, đơn vị có liên quan 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.

Chương II
NGUYÊN TẮC, CHẾ ĐỘ LÀM VIỆC VÀ KINH PHÍ HOẠT ĐỘNG

Điều 4. Nguyên tắc hoạt động của Đội ứng cứu

1. Điều phối hoạt động ứng cứu sự cố, tổ chức, phối hợp, hỗ trợ các Sở, ban, ngành, Ủy ban nhân dân các quận, huyện, đơn vị sự nghiệp trực thuộc Ủy ban nhân dân thành phố, các đoàn thể chính trị xã hội thành phố và các cơ quan Trung ương đóng trên địa bàn thành phố trong công tác ứng cứu sự cố an toàn thông tin mạng.

2. Tổ chức ứng cứu sự cố ATTTM phải đúng quy trình ứng cứu sự cố, dựa trên tính chất, mức độ, phạm vi và nguyên nhân xảy ra sự cố; bảo đảm nhanh chóng, chính xác, kịp thời, hiệu quả và an toàn thông tin.

3. Thông tin được trao đổi, cung cấp trong quá trình điều phối, xử lý sự cố phải được bảo đảm bí mật.

4. Thành viên Đội ứng cứu sự cố có quyền được chia sẻ thông tin, kinh nghiệm, tham gia các hoạt động diễn tập ứng cứu sự cố, tham gia các khóa đào tạo, bồi dưỡng về ATTTM và ứng cứu sự cố.

Điều 5. Chế độ làm việc của Đội ứng cứu

1. Các thành viên làm việc theo chế độ kiêm nhiệm. Khi xảy ra sự cố phải ưu tiên cho hoạt động của Đội ứng cứu sự cố, thực hiện nghiêm túc sự triệu tập, điều phối của Đội trưởng hoặc Đội phó khi được ủy quyền.

2. Thường trực Đội ứng cứu sự cố giúp Đội trưởng và các Đội phó trong hoạt động điều phối, ứng cứu sự cố.

3. Đội trưởng triệu tập thành viên Đội ứng cứu sự cố, tổ chức phiên họp thường kỳ 06 tháng/lần hoặc triệu tập họp đột xuất theo yêu cầu nhiệm vụ và yêu cầu của cơ quan cấp trên. Thời gian và địa điểm họp do Đội trưởng quyết định.

4. Đội trưởng triệu tập và điều phối các thành viên khi có sự cố xảy ra; khi vắng mặt, ủy quyền cho 01 Đội phó thực hiện thẩm quyền của mình. Đội phó khi được ủy quyền được sử dụng thẩm quyền của Đội trưởng để điều phối các hoạt động và chịu trách nhiệm về các quyết định của mình trước Đội trưởng và trước pháp luật.

5. Thẩm quyền ký ban hành văn bản của Đội ứng cứu sự cố thực hiện theo quy định của pháp luật hoặc theo phân công, ủy quyền:

a) Đội trưởng ký ban hành tất cả các văn bản của Đội ứng cứu sự cố theo thẩm quyền;

b) Đội phó Thường trực ký ban hành văn bản theo sự phân công của Đội trưởng.

Điều 6. Kinh phí hoạt động của Đội ứng cứu

Kinh phí hoạt động của Đội ứng cứu sự cố ATTTM thành phố Hồ Chí Minh được cấp theo quy định hiện hành.

Chương III
HOẠT ĐỘNG ĐIỀU PHỐI ỨNG CỨU SỰ CỐ

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

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 các thành viên, đơn vị có liên quan.

3. Xây dựng, nâng cao năng lực cho các thành viên 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 Đội ứng cứu sự cố và triển khai các hoạt động khác liên quan đến điều phối, ứng cứu sự cố, bảo đảm an toàn thông tin mạng

Điều 8. 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, Đội ứng cứu sự cố ATTTM, Sở Thông tin và Truyền thông. 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 báo cáo ngay cho Chủ quản hệ thống

thông tin, Đội ứng cứu sự cố ATTTM và Sở Thông tin và Truyền thông; 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 Sở Thông tin và Truyền thông;

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, Đội ứng cứu sự cố ATTTM, Sở Thông tin và Truyền thông.

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 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông;

c) Báo cáo diễn biến tình hình;

d) Báo cáo phương án ứng cứu cụ thể;

e) Báo cáo đề nghị hỗ trợ, phối hợp;

f) Báo cáo kết thúc ứng phó sự cố, nội dung theo Biểu mẫu số 04 Phụ lục I Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông.

4. Thường trực Đội ứng cứu sự cố tiếp nhận được thông báo sự cố phải báo cáo ngay cho Đội trưởng.

5. Đội trưởng quyết định điều phối các thành viên trong Đội; triệu tập cuộc họp (nếu cần); huy động các nguồn lực để xử lý sự cố khi cần thiết.

Điều 9. Hoạt động điều phối ứng cứu sự cố

1. Tuân thủ các nguyên tắc quy định tại Điều 4 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông.

2. 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;

e) 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;

f) 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 chỉ đạo của Ủy ban nhân dân thành phố, Bộ Thông tin và Truyền thông.

3. Đội trưởng hoặc Đội phó Thường trực thực hiện thông báo triệu tập, điều phối bằng văn bản đến các thành viên trong Đội ứng cứu sự cố. Trường hợp khẩn cấp có thể thông báo bằng điện thoại, email công vụ để điều phối và thông báo bằng văn bản sau.

Thường trực Đội ứng cứu sự cố thông báo cho các tổ chức, cá nhân gặp sự cố về yêu cầu phối hợp trong quá trình thực hiện điều phối và ứng cứu sự cố.

4. Thành viên Đội ứng cứu sự cố tiếp nhận thông báo điều phối; phối hợp chặt chẽ với đơn vị xảy ra sự cố và các thành viên cùng tham gia ứng cứu tổ chức thực hiện hoạt động ứng cứu theo quy trình tại Phụ lục I; báo cáo kết quả thực hiện cho Đội trưởng (thông qua Thường trực Đội ứng cứu sự cố).

5. Công tác ứng cứu kết thúc khi sự cố được khắc phục và hệ thống hoạt động trở lại bình thường.

6. Sau khi khắc phục sự cố, thành viên tham gia ứng cứu phải có trách nhiệm:

a) Rà soát, xác định nguyên nhân cơ bản gây ra sự cố;

b) Tổ chức kiểm tra lại và tham mưu giải pháp khắc phục triệt để sự cố;

c) Bảo đảm hệ thống hoạt động bình thường trước khi bàn giao hệ thống cho cơ quan, đơn vị chủ quản.

7. Thường trực Đội ứng cứu phải lưu trữ thông báo sự cố và biên bản xử lý sự cố; lưu trữ thông báo điều phối và báo cáo kết quả thực hiện khắc phục sự cố trong thời gian tối thiểu 01 năm.

Chương IV
TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Điều 10. Thông tin tiếp nhận

Đội ứng cứu là đầu mối liên lạc, tiếp nhận thông tin điều phối ứng cứu sự cố ATTTM của thành phố; các phản ánh sự cố, điều phối xử lý sự cố từ Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - VNCERT; giúp Đội trưởng Đội ứng cứu điều phối ứng cứu sự cố trên địa bàn thành phố Hồ Chí Minh.

Số điện thoại hotline 24/7: 0889490111

Số điện thoại thường trực: 38233717 ext: 111;

Email: ATTT@tphcm.gov.vn.

Điều 11. Trách nhiệm và quyền hạn của Đội trưởng Đội ứng cứu

1. Đội trưởng Đội ứng cứu chịu trách nhiệm trước Ủy ban nhân dân thành phố về toàn bộ hoạt động của Đội ứng cứu; kịp thời báo cáo, đề xuất Ủy ban nhân dân thành phố xem xét, chỉ đạo, giải quyết những công việc vượt thẩm quyền được giao, chủ trì các cuộc họp, điều phối, quyết định tổ chức ứng cứu; triệu tập các thành viên để xử lý và khắc phục sự cố ATTTM.

2. Chủ trì tổ chức ứng cứu sự cố ATTTM trên địa bàn thành phố. Là đầu mối liên hệ, phối hợp với Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - VNCERT, các doanh nghiệp cung cấp dịch vụ Internet và các đơn vị liên quan.

3. Quyết định hình thức điều phối các hoạt động ứng cứu sự cố và chịu trách nhiệm về các yêu cầu điều phối.

Điều 12. Trách nhiệm và quyền hạn của Đội phó thường trực

1. Giúp Đội trưởng điều hành các hoạt động của Đội ứng cứu sự cố, chịu trách nhiệm trước Đội trưởng về nhiệm vụ được giao; đề xuất kế hoạch, biện pháp kỹ thuật tăng cường công tác đảm bảo ATTTM.

2. Chỉ đạo các thành viên trong các hoạt động phòng ngừa, ngăn chặn và xử lý sự cố mạng máy tính theo thẩm quyền và nhiệm vụ được phân công; thay mặt Đội trưởng điều hành các hoạt động của Đội ứng cứu sự cố khi được ủy quyền.

3. Thực hiện các nhiệm vụ do Đội trưởng phân công và tham gia xây dựng kế hoạch hoạt động hàng năm của Đội ứng cứu.

Điều 13. Trách nhiệm và quyền hạn của các thành viên Đội ứng cứu sự cố

1. Thực hiện những nhiệm vụ do Đội trưởng giao.

2. Tiếp nhận và xử lý các thông báo sự cố hoặc văn bản triệu tập xử lý sự cố từ Đội trưởng.

3. Tham gia đầy đủ các cuộc họp định kỳ, đột xuất và hoạt động ứng cứu sự cố khi được triệu tập, điều phối của Đội trưởng.

4. Kịp thời báo cáo, đề xuất giải quyết những khó khăn, vướng mắc trong quá trình thực hiện nhiệm vụ cho Đội trưởng hoặc Đội phó để kịp thời có sự chỉ đạo, xử lý.

5. Phối hợp, hỗ trợ các thành viên khác trong Đội ứng cứu sự cố, cán bộ phụ trách CNTT của các cơ quan trong việc áp dụng các biện pháp, giải pháp kỹ thuật nhằm bảo đảm ATTTM cho các hệ thống thông tin, hệ thống máy tính, phòng chống sự cố mạng tại cơ quan, đơn vị.

6. Tiếp nhận đầy đủ, chính xác thông tin về sự cố được quy định tại khoản 4 Điều 9 Quy chế này và thông báo kịp thời cho Đội trưởng để thực hiện công tác điều phối ứng cứu sự cố.

7. Tham gia góp ý, đề xuất xây dựng Kế hoạch hoạt động hàng năm của Đội ứng cứu sự cố; tham gia các hoạt động diễn tập ứng cứu sự cố, các khóa đào tạo, bồi dưỡng về an toàn thông tin và ứng cứu sự cố do Sở Thông tin và Truyền thông triệu tập.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 14. Điều khoản thi hành

1. Thủ trưởng các cơ quan, đơn vị có trách nhiệm tạo mọi điều kiện cho cán bộ là thành viên Đội ứng cứu sự cố và các bộ phận có liên quan thực hiện tốt Quy chế này.

2. Các đơn vị có liên quan kịp thời thông báo về Sở Thông tin và Truyền thông khi có thay đổi thành viên Đội ứng cứu sự cố.

3. Các thành viên Đội ứng cứu sự cố và cá nhân có liên quan thực hiện nghiêm túc Quy định này.

4. Trong quá trình thực hiện Quy định, nếu có vấn đề cần sửa đổi, bổ sung, các thành viên kịp thời phản ánh về Sở Thông tin và Truyền thông để nghiên cứu,

xem xét, điều chỉnh, bổ sung cho phù hợp với tình hình thực tế./.

Phụ lục I

Quy trình ứng cứu sự cố

(Ban hành kèm theo Quy định về hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng Thành phố Hồ Chí Minh)

Thành phần	Quy trình	Ghi chú
- Đơn vị chủ quản, đơn vị, cá nhân vận hành HTTT	Phát hiện, tiếp nhận thông tin sự cố	Thông tin sự cố có thể từ các nguồn: - Hệ thống theo dõi nội bộ của đơn vị vận hành; - Đơn vị cung cấp dịch vụ/ sản phẩm (hạ tầng, đường truyền, phần mềm)
- Đơn vị chủ quản, đơn vị, cá nhân vận hành HTTT, đơn vị chuyên trách ứng cứu sự cố/ đơn vị chuyên trách CNTT	Phân tích, xác minh sự cố Chưa xảy ra → Phản hồi, kết thúc Đã xảy ra	Đơn vị phối hợp: Đơn vị cung cấp dịch vụ/ sản phẩm (hạ tầng, đường truyền, phần mềm)
- Đơn vị chủ quản, đơn vị, cá nhân vận hành HTTT, đơn vị chuyên trách ứng cứu sự cố/ đơn vị chuyên trách CNTT triển khai các bước ứng cứu ban đầu; báo cáo sự cố	Lựa chọn phương án, ứng cứu ban đầu Hoàn thành → Phản hồi, kết thúc Chưa hoàn thành Báo cáo sự cố cho Đội ứng cứu	- Đơn vị phối hợp: Đơn vị cung cấp dịch vụ/ sản phẩm (hạ tầng, đường truyền, phần mềm) - Các đơn vị phối hợp 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 ứng cứu sự cố/ đơn vị chuyên trách CNTT ứng cứu ban đầu sự cố trong 2 giờ kể từ lúc phát hiện sự cố. Nếu sau 2 giờ chưa kết thúc sự cố, báo ngay cho Đội ứng cứu sự cố ATTT (*)
- Đội ứng cứu sự cố ATTT - Đơn vị chủ quản, đơn vị, cá nhân vận hành HTTT, đơn vị chuyên trách ứng cứu sự cố/ đơn vị chuyên trách CNTT - Các cá nhân/ đơn vị khác có liên quan	Điều phối, chỉ đạo công tác ứng cứu sự cố Thu thập, phân tích, xác định sự cố Ứng cứu, xử lý sự cố Chưa hoạt động bình thường Kiểm tra đánh giá Khôi phục hoạt động	- Đơn vị phối hợp: Đơn vị cung cấp dịch vụ/ sản phẩm (hạ tầng, đường truyền, phần mềm) - Các thành phần tham gia ứng cứu sự cố căn cứ 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 phục hoạt động của hệ thống thông tin trở lại bình thường
- Đội ứng cứu sự cố ATTT - Đơn vị chủ quản, đơn vị, cá nhân vận hành HTTT, đơn vị chuyên trách ứng cứu sự cố/ đơn vị chuyên trách CNTT - Các cá nhân/ đơn vị khác có liên quan	Đã hoạt động bình thường Tổng kết, đánh giá	

(*) Đối với các sự cố trên Trung tâm dữ liệu thành phố, đơn vị cung cấp dịch vụ/ sản phẩm (hạ tầng, đường truyền, phần mềm) phải báo cáo ngay cho Đội ứng cứu sự cố ATTT trước khi tiến hành ứng cứu ban đầu