BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 27/2011/TT-BTTTT	*Hà Nội, ngày 4 tháng 10 năm 2011*

THÔNG TƯ
Quy định về điều phối các hoạt động ứng cứu sự cố mạng Internet Việt Nam

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

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

Căn cứ Luật Viễn thông ngày 04 tháng 12 năm 2009;

Căn cứ Nghị định số 64/2007/NĐ-CP ngày 10 tháng 4 năm 2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước;

Căn cứ Nghị định số 97/2008/NĐ-CP ngày 28 tháng 8 năm 2008 về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin điện tử trên Internet;

Căn cứ Nghị định số 187/2007/NĐ-CP ngày 25 tháng 12 năm 2007 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

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

QUY ĐỊNH:

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

Thông tư này quy định về mạng lưới ứng cứu sự cố, điều phối các hoạt động ứng cứu sự cố mạng Internet; trách nhiệm của các tổ chức, cá nhân có liên quan tới hoạt động ứng cứu sự cố mạng Internet tại Việt Nam.

Điều 2. Giải thích thuật ngữ

1. Sự cố mạng Internet là sự kiện đã, đang hoặc có khả năng xảy ra gây mất an toàn thông tin trên mạng Internet được phát hiện thông qua việc giám sát,

đánh giá, phân tích của các cơ quan, tổ chức, cá nhân có liên quan hoặc được cảnh báo từ các chuyên gia, tổ chức về lĩnh vực an toàn thông tin trong nước và trên thế giới (sau đây được gọi tắt là sự cố).

2. Sự cố có tính chất nghiêm trọng là sự cố có một hoặc nhiều tính chất sau: có khả năng xảy ra trên diện rộng, lan nhanh; có khả năng phá hoại hệ thống mạng máy tính và mạng Internet; có thể gây thiệt hại hay hậu quả lớn cho các hệ thống thông tin trên mạng; đòi hỏi phối hợp nhiều nguồn lực lớn của quốc gia hay của quốc tế để giải quyết.

Chương II
MẠNG LƯỚI ỨNG CỨU SỰ CỐ

Điều 3. Mạng lưới ứng cứu sự cố

1. Mạng lưới ứng cứu sự cố là tập hợp các cơ quan, tổ chức, doanh nghiệp tham gia hoạt động ứng cứu sự cố có sự điều phối tại Việt Nam (sau đây gọi tắt là mạng lưới, các cơ quan, tổ chức, doanh nghiệp gọi chung là thành viên mạng lưới và gọi tắt là thành viên). Mạng lưới bao gồm các thành viên có nghĩa vụ tham gia mạng lưới và thành viên tự nguyện đăng ký tham gia mạng lưới.

2. Thành viên có nghĩa vụ tham gia mạng lưới gồm có:

a) Cơ quan điều phối;

b) Đơn vị chuyên trách về công nghệ thông tin của các Bộ, Cơ quan ngang Bộ, Cơ quan thuộc Chính phủ; Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương;

c) Các doanh nghiệp cung cấp dịch vụ Internet (ISP);

d) Trung tâm Internet Việt Nam (VNNIC).

3. Thành viên tự nguyện tham gia mạng lưới là cơ quan, tổ chức hay doanh nghiệp tự nguyện tham gia hoạt động trong mạng lưới có bản khai đăng ký theo mẫu tại Phụ lục 1 gửi tới Cơ quan điều phối và được chấp nhận. Khuyến khích các tổ chức hoạt động trong lĩnh vực an toàn thông tin thành lập các bộ phận có chức năng ứng cứu sự cố và tham gia vào mạng lưới.

4. Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (Trung tâm VNCERT) là Cơ quan điều phối. Trung tâm VNCERT thực hiện chức năng điều phối các hoạt động ứng cứu sự cố trên toàn quốc và có quyền điều động các tổ chức khác trong mạng lưới phối hợp ngăn chặn, xử lý và khắc phục sự cố mạng Internet tại Việt Nam; có quyền quyết định hình thức điều phối các hoạt động ứng cứu sự cố và chịu trách nhiệm về các yêu cầu điều phối; là đầu mối trao đổi thông tin về hợp tác ứng cứu sự cố với các tổ chức ứng cứu khẩn cấp máy tính quốc tế. Hoạt

động của Cơ quan điều phối nhằm điều động các thành viên mạng lưới phối hợp xử lý, ứng cứu sự cố gọi là điều phối ứng cứu sự cố.

5. Thông tin liên lạc chi tiết về địa chỉ, số điện thoại, số fax, địa chỉ thư điện tử, trang tin điện tử của thành viên mạng lưới được công bố công khai trên trang tin điện tử của Cơ quan điều phối (www.vncert.gov.vn).

Điều 4. Đầu mối ứng cứu sự cố

1. Đầu mối ứng cứu sự cố là cá nhân hay bộ phận được phép thay mặt cho thành viên mạng lưới để liên lạc và trao đổi thông tin với các thành viên mạng lưới khác trong hoạt động ứng cứu sự cố.

2. Đầu mối ứng cứu sự cố phải có trình độ chuyên môn và kỹ năng nghiệp vụ để thực hiện các hoạt động phối hợp ứng cứu sự cố.

3. Đầu mối ứng cứu sự cố phải bảo đảm khả năng liên lạc thông suốt liên tục (24 giờ trong một ngày và 7 ngày trong tuần).

Điều 5. Nguyên tắc hoạt động của mạng lưới ứng cứu sự cố

1. Thông tin được trao đổi, cung cấp trong quá trình điều phối, xử lý sự cố phải được bảo đảm bí mật theo yêu cầu của tổ chức, cá nhân gặp sự cố trừ khi sự cố xảy ra có liên quan tới nhiều đối tượng người dùng khác mà Cơ quan điều phối có yêu cầu cảnh báo, nhắc nhở.

2. Việc trao đổi thông tin trong mạng lưới phải được thực hiện bằng một hoặc nhiều hình thức như: công văn, thư điện tử, điện thoại, fax. Thành viên mạng lưới tiếp nhận được thông tin phải chủ động xác thực đối tượng gửi nhằm bảo đảm thông điệp nhận được là tin cậy.

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

Điều 6. Chế độ báo cáo

1. Thành viên mạng lưới có trách nhiệm báo cáo định kỳ 6 tháng một lần cho Cơ quan điều phối về hoạt động tiếp nhận và xử lý sự cố.

a) Nội dung báo cáo theo mẫu báo cáo định kỳ tại Phụ lục 2. Hướng dẫn mẫu báo cáo đăng trên trang tin điện tử của Trung tâm VNCERT;

b) Thời gian gửi báo cáo: trước ngày 15 tháng 6 và trước ngày 15 tháng 12 hàng năm;

c) Hình thức báo cáo: bằng công văn và thư điện tử;

d) Báo cáo gửi về Trung tâm VNCERT: 18 Nguyễn Du, Hà Nội; địa chỉ thư điện tử: baocao@vncert.vn.

2. Thành viên mạng lưới có trách nhiệm báo cáo đột xuất khi có yêu cầu của Cơ quan điều phối hoặc khi phát hiện ra các sự cố có tính chất nghiêm trọng. Hình thức và địa chỉ gửi báo cáo theo quy định tại khoản 1 Điều này.

Chương III
ĐIỀU PHỐI CÁC HOẠT ĐỘNG ỨNG CỨU SỰ CỐ

Điều 7. Thông báo sự cố

1. Khi gặp sự cố mà không tự khắc phục được, tổ chức hay cá nhân sử dụng Internet thông báo sự cố tới một hoặc nhiều thành viên mạng lưới sau:

a) Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân đó (nếu có);

b) Các ISP đang trực tiếp cung cấp dịch vụ Internet cho tổ chức, cá nhân đó;

c) Cơ quan điều phối.

2. Khi phát hiện thấy các sự cố có tính chất nghiêm trọng, tổ chức, cá nhân phải thông báo ngay cho Cơ quan điều phối.

3. Nội dung thông báo sự cố gồm:

a) Thông tin mô tả sự cố theo mẫu thông báo sự cố tại Phụ lục 3;

b) Thông tin khác theo yêu cầu của đơn vị tiếp nhận thông báo.

4. Hướng dẫn chi tiết thông báo sự cố đăng tại trang tin điện tử của Cơ quan điều phối.

5. Tổ chức, cá nhân gửi thông báo sự cố phải phối hợp chặt chẽ, cung cấp đầy đủ và chính xác thông tin về sự cố cho các thành viên mạng lưới tiếp nhận thông báo sự cố và tạo mọi điều kiện thuận lợi cho các thành viên này và Cơ quan điều phối tiếp cận, nghiên cứu hệ thống, thiết bị liên quan đến sự cố để thu thập, phân tích thông tin xử lý sự cố.

Điều 8. Tiếp nhận và xử lý thông báo sự cố

1. Thành viên mạng lưới tiếp nhận thông báo sự cố phải thực hiện:

a) Phản hồi ngay và không vượt quá 24 giờ cho tổ chức, cá nhân gửi thông báo để xác nhận về việc đã nhận được thông báo sự cố;

b) Xử lý sự cố trong khả năng và trách nhiệm của mình;

c) Thông báo sự cố về Cơ quan điều phối trong trường hợp không xử lý được.

2. Cơ quan điều phối tiếp nhận được thông báo sự cố phải thực hiện:

a) Các hoạt động xử lý sự cố với tư cách thành viên mạng lưới như quy định tại khoản 1 Điều này;

b) Đưa ra yêu cầu điều phối tới thành viên mạng lưới tham gia ứng cứu sự cố khi cần thiết;

c) Huy động các nguồn lực khác, mời chuyên gia tham gia ứng cứu sự cố khi cần thiết;

d) Tổ chức hoạt động phối hợp với các tổ chức ứng cứu sự cố máy tính quốc tế để ứng cứu các sự cố có phạm vi xuyên biên giới.

Điều 9. Điều phối ứng cứu sự cố

1. Cơ quan điều phối thực hiện việc điều phối bằng cách gửi yêu cầu điều phối tới các thành viên mạng lưới có liên quan tới sự cố, sử dụng mẫu biểu yêu cầu điều phối theo Phụ lục 4.

2. Cơ quan điều phối có quyền yêu cầu các thành viên mạng lưới hợp tác và đề nghị các tổ chức ứng cứu khẩn cấp máy tính quốc tế tham gia hoạt động ứng cứu sự cố.

3. Cơ quan điều phối 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 mạng lưới tiếp nhận yêu cầu điều phối, thực hiện đúng yêu cầu điều phối và báo cáo, phản hồi đầy đủ kết quả thực hiện cho Cơ quan điều phối.

Chương IV
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC, CÁ NHÂN

Điều 10. Thành viên mạng lưới

1. Công bố địa chỉ tiếp nhận thông báo sự cố trên trang tin điện tử của mình.

2. Cử nhân sự làm Đầu mối ứng cứu sự cố và bảo đảm Đầu mối tuân thủ đúng quy định tại Điều 4.

3. Tiếp nhận và xử lý các thông báo sự cố theo quy định tại Điều 8.

4. Tuân thủ các yêu cầu điều phối của Cơ quan điều phối theo quy định tại Điều 9.

5. Phối hợp, hỗ trợ các thành viên mạng lưới khác trong các hoạt động ứng cứu sự cố.

6. Thông báo và cập nhật cho Cơ quan điều phối các thông tin sau:

a) Địa chỉ tiếp nhận thông báo sự cố;

b) Thông tin về Đầu mối ứng cứu sự cố bao gồm: họ tên, chức vụ, địa chỉ liên hệ, số điện thoại cố định, số điện thoại di động, số fax, địa chỉ thư điện tử.

7. Lưu trữ thông báo sự cố và biên bản xử lý sự cố, lưu trữ yêu cầu điều phối và báo cáo kết quả thực hiện yêu cầu điều phối trong thời gian tối thiểu 01 năm, bao gồm các thông tin sau:

a) Nội dung thông báo sự cố, thời gian tiếp nhận thông báo, thời gian gửi xác nhận;

b) Kết quả xử lý sự cố, nguyên nhân gây ra sự cố, thời gian xử lý sự cố và danh sách các tổ chức, cá nhân cùng tham gia phối hợp xử lý sự cố (nếu có);

c) Thời gian gửi thông báo sự cố cho Cơ quan điều phối, thời gian nhận được xác nhận từ Cơ quan điều phối đối với trường hợp thông báo cho Cơ quan điều phối.

8. Thực hiện chế độ báo cáo theo quy định tại Điều 6.

Điều 11. Cơ quan điều phối (Trung tâm VNCERT)

1. Thực hiện nghĩa vụ thành viên mạng lưới theo quy định tại khoản 1,2,3,5,7 Điều 10, trong đó thời hạn lưu trữ tài liệu đối với khoản 7 Điều 10 thực hiện theo quy định hiện hành của Nhà nước về thời hạn bảo quản hồ sơ, tài liệu hình thành phổ biến trong hoạt động của cơ quan nhà nước.

2. Tổ chức hoạt động cho mạng lưới và điều phối hoạt động ứng cứu sự cố, xây dựng các quy định, hướng dẫn trong mạng lưới về ứng cứu sự cố.

3. Tiếp nhận, xử lý trực tiếp hoặc điều phối xử lý các thông báo sự cố.

4. Xây dựng và triển khai hệ thống kỹ thuật hỗ trợ cho hoạt động liên lạc, trao đổi thông tin trong mạng lưới và tạo điều kiện cho các thành viên mạng lưới sử dụng hệ thống.

5. Tổng hợp và công bố trong mạng lưới các thông tin thông báo, cảnh báo về các điểm yếu, lỗ hổng, các nguồn tấn công trên mạng Internet.

6. Tập hợp, cập nhật và công bố trên trang tin điện tử của Trung tâm VNCERT thông tin về các địa chỉ tiếp nhận thông báo sự cố của các thành viên mạng lưới.

7. Tập hợp, cập nhật và công bố thông tin về danh sách các đầu mối cho các thành viên mạng lưới.

8. Cung cấp báo cáo thống kê hàng năm về hoạt động ứng cứu khẩn cấp sự cố.

Điều 12. Doanh nghiệp cung cấp dịch vụ Internet

1.Thực hiện nghĩa vụ thành viên mạng lưới theo quy định tại Điều 10.

2.Hướng dẫn người sử dụng dịch vụ Internet hoặc thuê bao Internet (sau đây gọi chung là khách hàng) thực hiện thông báo sự cố.

3.Thực hiện chức năng xử lý sự cố cho khách hàng khi tiếp nhận được thông báo hoặc phát hiện được sự cố.

4.Cung cấp các thông tin sau khi Cơ quan điều phối có yêu cầu:

a) Thông tin về khách hàng của mình có liên quan tới sự cố, thông tin kỹ thuật về hệ thống của khách hàng có liên quan tới sự cố (địa chỉ IP, tên miền, nhật ký truy nhập, các thông tin khác nếu có);

b) Thông tin cấu trúc mạng, thông tin giám sát, thống kê về các luồng dữ liệu mạng liên quan tới sự cố (nếu có);

c) Cung cấp phần mềm, mã nguồn phần mềm gây ra sự cố, dữ liệu lưu trữ liên quan tới sự cố, thông tin về phần cứng gây ra sự cố (nếu có).

5. Lắp đặt sẵn các cổng kết nối, giao diện kết nối dự phòng tại các điểm kết nối Internet quan trọng để phục vụ cho chính mình và cho các cơ quan nhà nước có thẩm quyền thực hiện giám sát, phát hiện các cuộc tấn công hoặc sự phát tán, lan truyền của phần mềm mã độc.

6. Tạo điều kiện cho Cơ quan điều phối tiếp cận, nghiên cứu hệ thống, thiết bị liên quan đến sự cố để thu thập, phân tích thông tin nhằm mục đích xử lý sự cố.

7. Thực hiện theo yêu cầu điều phối các hoạt động sau đây:

a) Ngừng kết nối với thiết bị, hệ thống dịch vụ gây ra sự cố;

b) Ngăn chặn, chuyển hướng tạm thời các địa chỉ IP, tên miền gây ra sự cố;

c) Gỡ bỏ hoặc gỡ bỏ tạm thời các ứng dụng, dịch vụ gây ra sự cố trên mạng Internet.

8. Hỗ trợ các nguồn lực trong khả năng của mình và trong khoảng thời gian xác định theo yêu cầu của Cơ quan điều phối nhằm thực hiện hoạt động ứng cứu sự cố hoặc diễn tập ứng cứu sự cố, bao gồm:

a) Đường truyền kết nối Internet đối với trường hợp xảy ra sự cố tấn công từ chối dịch vụ làm cạn kiệt tài nguyên băng thông hoặc cần tăng cường tính sẵn sàng cho các hệ thống cung cấp dịch vụ quan trọng;

b) Nhân lực về an toàn thông tin tham gia hoạt động ứng cứu sự cố;

c) Thiết bị, công nghệ về an toàn thông tin (nếu có).

Điều 13. Trung tâm VNNIC

1. Thực hiện nghĩa vụ thành viên mạng lưới theo quy định tại Điều 10.

2. Cung cấp thông tin chủ thể đăng ký tên miền quốc gia (.vn), đơn vị quản lý địa chỉ IP, số hiệu mạng do VNNIC cấp và các thông tin khác có liên quan tới sự cố theo yêu cầu của Cơ quan điều phối.

3. Thực hiện các yêu cầu điều phối của Cơ quan điều phối về việc xử lý các sự cố liên quan đến tài nguyên Internet của Việt Nam.

Điều 14. Đơn vị chuyên trách về công nghệ thông tin của các Bộ, Cơ quan ngang Bộ, Cơ quan thuộc Chính phủ; Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương

1. Thực hiện nghĩa vụ thành viên mạng lưới theo quy định tại Điều 10.

2. Xây dựng và hướng dẫn việc thực hiện hoạt động ứng cứu sự cố trong phạm vi trách nhiệm của đơn vị.

3. Phối hợp, hỗ trợ hoạt động ứng cứu khẩn cấp sự cố trong phạm vi trách nhiệm và địa bàn hoạt động của đơn vị khi có yêu cầu từ Cơ quan điều phối.

Điều 15. Các cá nhân, tổ chức khác

1. Các tổ chức cung cấp dịch vụ an toàn thông tin

a) Chia sẻ thông tin và số liệu về hoạt động ứng cứu sự cố đã thực hiện khi có yêu cầu của Cơ quan điều phối;

b) Hỗ trợ về nhân lực, giải pháp công nghệ theo khả năng khi có yêu cầu của Cơ quan điều phối.

2. Các tổ chức, cá nhân sử dụng mạng Internet

a) Chủ động áp dụng các biện pháp, giải pháp kỹ thuật bảo đảm an toàn thông tin, rà quét mã độc trong máy tính nhằm phòng chống sự cố mạng Internet;

b) Chủ động cung cấp thông tin và tích cực phối hợp với các thành viên mạng lưới ứng cứu sự cố trong hoạt động phát hiện, ngăn chặn và xử lý sự cố.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 16. Hiệu lực thi hành

1. Thông tư này có hiệu lực thi hành kể từ ngày 15 tháng 11 năm 2011.

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

Nơi nhận:
- Thủ tướng Chính phủ, các PTTgCP (để b/c);
- Văn phòng Quốc hội;
- Văn phòng Chủ tịch nước;
- Văn phòng TW và các Ban của Đảng;
- Các Bộ và cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Toà án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- UBND các tỉnh, thành phố trực thuộc TW;
- Cơ quan Trung ương của các đoàn thể;
- Ban Chỉ đạo quốc gia về CNTT;
- Ban Chỉ đạo CNTT của cơ quan Đảng;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc TW;
- Công báo, Cổng Thông tin điện tử Chính phủ;
- Cục Kiểm tra VBQPPL (Bộ Tư pháp);
- Bộ TTTT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ, Cổng Thông tin điện tử;
- Lưu: VT, VNCERT (5b).

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nguyễn Minh Hồng

PHỤ LỤC 1: MẪU BẢN KHAI ĐĂNG KÝ THAM GIA MẠNG LƯỚI ĐIỀU PHỐI

TÊN TỔ CHỨC
.....

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

BẢN KHAI ĐĂNG KÝ THAM GIA MẠNG LƯỚI ĐIỀU PHỐI ỨNG CỨU SỰ CỐ

1. Thông tin chung về tổ chức

- Tên tổ chức: .....
- Điện thoại: .....
- Fax: .....
- Email: .....
- Website: .....

2. Hoạt động trong lĩnh vực an toàn thông tin

☐ Có

☐ Không

3. Thông tin tiếp nhận thông báo sự cố

- Địa chỉ liên lạc: .....
- Email: .....
- Số điện thoại (cố định, di động).....
- Fax: .....

4. Đầu mối ứng cứu sự cố

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

5. Giới thiệu về hoạt động của tổ chức

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

.....

.....

.....

.....

.....

.....

.....

Tổ chức cam kết tuân thủ các quy định về hoạt động ứng cứu sự cố do Cơ quan điều phối ban hành.

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

Xác nhận của chủ thể đăng ký
(Đóng dấu hoặc sử dụng chữ ký số)

PHỤ LỤC 2: MẪU BÁO CÁO ĐỊNH KỲ

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

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

BÁO CÁO ĐỊNH KỲ VỀ HOẠT ĐỘNG TIẾP NHẬN VÀ XỬ LÝ SỰ CỐ

☐ Từ tháng ……/20 … đến tháng …./20…

Tên tổ chức/doanh nghiệp: .....

Địa chỉ: .....

1. Số lượng thông báo sự cố và cách thức xử lý

Loại sự cố	Số lượng	Số sự cố tự xử lý	Số sự cố có sự hỗ trợ xử lý từ các tổ chức khác	Số sự cố có hỗ trợ xử lý từ tổ chức nước ngoài	Số sự cố đề nghị VNCERT hỗ trợ xử lý	Thiệt hại ước tính
Từ chối dịch vụ						
Mã độc hại						
Thay đổi giao diện web						
Phishing						
Truy cập trái phép						
Sử dụng bất hợp lý						
Đa thành phần						
Khác						
Tổng số						

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

.....

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

.....

4. Đề xuất kiến nghị: .....

.....

....., ngày ..... tháng ..... năm .....
Giám đốc
(Đóng dấu hoặc sử dụng chữ ký số)

PHỤ LỤC 3: MẪU THÔNG BÁO KHI CÓ SỰ CỐ

THÔNG BÁO SỰ CỐ

- Cá nhân / tổ chức thông báo sự cố * .....
- Email * .....
- Điện thoại * .....

Thông tin về sự cố

- Mô tả sơ bộ về sự cố * .....

.....

- Cách thức phát hiện * *(Đánh dấu những cách thức được sử dụng để phát hiện sự cố)*
  - ☐ Qua hệ thống phát hiện xâm nhập ☐ Kiểm tra dữ liệu lưu lại (Log File)
  - ☐ Nhận được thông báo từ: .....
  - ☐ Khác, đó là .....
- Thời gian xảy ra sự cố *: .../.../...../.../... (ngày/tháng/năm/giờ/phút)

  (Ngày,Tháng điền đủ 2 chữ số,Năm điền đủ 4 chữ số,Giờ,Phút điền đủ 2 chữ số theo hệ 24 giờ)
- Thời gian thực hiện báo cáo sự cố *: .../.../...../.../... (ngày/tháng/năm/giờ/phút)

Đã gửi thông báo sự cố cho *

- ☐ Thành viên mạng lưới chịu trách nhiệm ứng cứu sự cố cho tổ chức, cá nhân
- ☐ ISP đang trực tiếp cung cấp dịch vụ
- ☐ Cơ quan điều phối

Thông tin về hệ thống xảy ra sự cố

- Hệ điều hành ..... Version .....
- Các dịch vụ có trên hệ thống *(Đánh dấu những dịch vụ được sử dụng trên hệ thống)*
  - ☐ Web server ☐ Mail server ☐ Database server
  - ☐ Dịch vụ khác, đó là .....
- Các biện pháp an toàn thông tin đã triển khai *(Đánh dấu những biện pháp đã triển khai)*
  - ☐ Antivirus ☐ Firewall ☐ Hệ thống phát hiện xâm nhập
  - ☐ Khác:.....
- Các địa chỉ IP của hệ thống *(Liệt kê địa chỉ IP sử dụng trên Internet, không liệt kê địa chỉ IP nội bộ)*

.....

- Các tên miền của hệ thống

.....

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

.....

- Thông tin gửi kèm
  - ☐ Nhật ký hệ thống ☐ Mẫu virus / mã độc ☐ Khác:.....
- Các thông tin cung cấp trong thông báo sự cố này đều phải được giữ bí mật: ☐ Có ☐ Không
- Sự cố đã được khắc phục: ☐ Đã khắc phục ☐ Chưa khắc phục (đề nghị ứng cứu)
- Kiến nghị .....

Cá nhân / Tổ chức thông báo

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

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

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

PHỤ LỤC 4: MẪU YÊU CẦU ĐIỀU PHỐI

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

Số: /VNCERT-NV
V/v Thực hiện yêu cầu điều phối

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

....., ngày..... tháng .... năm .....

Kính gửi: .....

Đề nghị thực hiện yêu cầu điều phối dưới đây:

1. Loại yêu cầu điều phối

☐ Thông báo nguy cơ, tình hình sự cố.

☐ Yêu cầu xử lý sự cố cụ thể

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

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

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

2. Tổ chức có liên quan tới sự cố

.....

.....

.....

3. Nội dung cụ thể yêu cầu điều phối

.....

.....

.....

.....

.....

.....

.....

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

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

Giám đốc
(Đóng dấu hoặc sử dụng chữ ký số)