BỘ Y TẾ	CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
	Độc lập - Tự do - Hạnh phúc
Số: 4494 /QĐ-BYT	*Hà Nội, ngày 30 tháng 10 năm 2015*

QUYẾT ĐỊNH

Ban hành Quy trình phản ứng với các sự cố an toàn, an ninh thông tin tại các đơn vị trong ngành y tế

BỘ TRƯỞNG BỘ Y TẾ

Căn cứ Nghị định số 63/2012/NĐ-CP ngày 31/8/2012 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Y tế;

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

Căn cứ Thông tư số 53/2014/TT-BYT ngày 29/12/2014 của Bộ Y tế quy định điều kiện hoạt động y tế trên môi trường mạng;

Căn cứ Quyết định số 4159/QĐ-BYT ngày 13/10/2014 của Bộ Y tế ban hành Quy định về đảm bảo an toàn thông tin y tế điện tử tại các đơn vị trong ngành y tế;

Xét đề nghị của Cục trưởng Cục Công nghệ thông tin,

QUYẾT ĐỊNH:

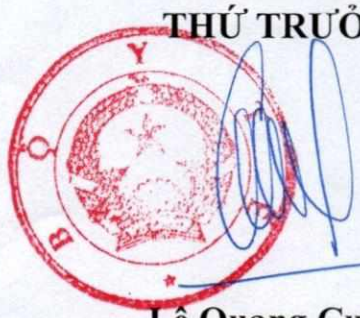
Điều 1. Ban hành kèm theo quyết định này "Quy trình phản ứng với các sự cố an toàn, an ninh thông tin tại các đơn vị trong ngành y tế".

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

Điều 3. Chánh văn phòng Bộ, Cục trưởng Cục Công nghệ thông tin, Thủ trưởng các đơn vị thuộc/trực thuộc Bộ Y tế và tổ chức liên quan chịu trách nhiệm thi hành quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ trưởng Bộ Y tế (để b/c);
- Các Thứ trưởng Bộ Y tế (để phối hợp chỉ đạo);
- Sở Y tế các tỉnh/thành phố trực thuộc TW;
- Cổng Thông tin điện tử Bộ Y tế;
- Lưu: VT, CNTT (2).

KT. BỘ TRƯỞNG
THỨ TRƯỞNG



Lê Quang Cường

BỘ Y TẾ

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

QUY TRÌNH

Phản ứng với các sự cố an toàn, an ninh thông tin tại các đơn vị trong ngành y tế

(Ban hành kèm theo Quyết định số 4494 /QĐ-BYT ngày 30 tháng 10 năm 2015 của Bộ trưởng Bộ Y tế)

Chương I
QUY ĐỊNH CHUNG

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

1. Quyết định này ban hành Quy trình quản lý, xử lý sự cố an toàn thông tin y tế trên môi trường mạng và trách nhiệm của tổ chức, cá nhân có liên quan tới hoạt động xử lý sự cố an toàn, an ninh thông tin y tế điện tử.

2. Quy trình này áp dụng đối với các đơn vị, tổ chức trong ngành y tế triển khai ứng dụng công nghệ thông tin trong quản lý, sử dụng, lưu trữ, truyền đưa thông tin trên môi trường mạng (sau đây gọi tắt là đơn vị).

Điều 2. Giải thích từ ngữ

Trong Quy trình này, các từ ngữ dưới đây được hiểu như sau:

1. *Sự cố an toàn, an ninh thông tin y tế*: là sự kiện đã, đang hoặc có khả năng xảy ra gây mất an toàn, an ninh thông tin y tế trên môi trường mạng; 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 cá nhân, tổ chức về lĩnh vực an toàn, an ninh thông tin (sau đây gọi tắt là sự cố).

2. *Hệ thống thông tin y tế (gọi tắt là hệ thống)*: là một tập hợp có cấu trúc các trang thiết bị phần cứng, phần mềm, cơ sở dữ liệu và hệ thống mạng phục vụ cho một hoặc nhiều hoạt động y tế trên môi trường mạng.

3. *Hệ thống đặc biệt quan trọng*: là hệ thống có ảnh hưởng đặc biệt quan trọng tới an ninh, xã hội, y tế nói chung; hoặc có ảnh hưởng đặc biệt quan trọng tới hoạt động của đơn vị.

4. *Hệ thống quan trọng*: là hệ thống thông tin y tế có ảnh hưởng đáng kể tới an ninh, xã hội, y tế nói chung; hoặc có ảnh hưởng đáng kể tới hoạt động của đơn vị.

5. *Hệ thống thông thường*: là hệ thống thông tin phục vụ các hoạt động thông thường của đơn vị, không ảnh hưởng tới an ninh, xã hội, y tế nói chung và không có ảnh hưởng đáng kể tới hoạt động của đơn vị.

6. *Bên liên quan*: là cá nhân, tổ chức cung cấp dịch vụ công nghệ thông tin liên quan tới sự cố hoặc chịu ảnh hưởng trực tiếp hoặc gián tiếp tới sự cố.

Điều 3. Phân loại sự cố

1. Các sự cố dưới đây cần được xem xét phân loại và xử lý, bao gồm:

a) Các truy cập trái phép, hành vi vi phạm tính bảo mật và tính toàn vẹn thông tin, dữ liệu y tế, ứng dụng triển khai trong ngành y tế;

b) Mã độc, tấn công từ chối dịch vụ;

c) Điểm yếu, lỗ hổng bảo mật của hạ tầng, hệ điều hành, ứng dụng;

d) Hệ thống trục trặc nhiều lần hoặc quá tải gây ảnh hưởng tới hoạt động của hệ thống;

đ) Các trục trặc của phần mềm hay phần cứng không khắc phục được gây ảnh hưởng đến hoạt động của hệ thống;

e) Mất thiết bị, phương tiện công nghệ thông tin;

g) Không tuân thủ chính sách an toàn thông tin hoặc các chỉ dẫn bắt buộc của đơn vị hoặc hành vi vi phạm an ninh vật lý;

h) Các sự cố liên quan tới các thảm họa thiên nhiên như núi lửa, động đất, lũ lụt, sấm sét;

i) Các sự cố khác gây gián đoạn, ảnh hưởng đến hoạt động bình thường của các ứng dụng công nghệ thông tin tại đơn vị.

2. Các sự cố cần được phân loại theo mức độ nghiêm trọng, bao gồm:

a) Mức 0 (không): sự cố không gây ảnh hưởng có hại tức thời đến hoạt động và dữ liệu của hệ thống. Tuy nhiên, cần phân tích và báo cáo lại để tránh phát sinh những sự cố khác trong tương lai.

b) Mức 1 (thấp): sự cố gây ảnh hưởng tới các hệ thống nói chung, gây ảnh hưởng nhỏ hoặc không đáng kể đến hoạt động của hệ thống hoặc dữ liệu của hệ thống, gây ra những tác động không đáng kể cho đơn vị hoặc cho xã hội.

c) Mức 2 (trung bình): sự cố gây ảnh hưởng tới các hệ thống quan trọng hoặc thông thường, gây ảnh hưởng đáng kể đến hoạt động hoặc dữ liệu của hệ thống, hoặc gây ra những tác động đáng kể cho đơn vị hoặc cho xã hội.

d) Mức 3 (nghiêm trọng): sự cố xảy ra đối với các hệ thống đặc biệt quan trọng hoặc các hệ thống quan trọng, gây ảnh hưởng nghiêm trọng đến hoạt động của hệ thống, bao gồm việc ngừng hoạt động trong một thời gian dài hoặc thiệt hại nghiêm trọng đến dữ liệu của hệ thống; hoặc gây đến những tác động nghiêm trọng cho đơn vị hoặc cho xã hội.

đ) Mức 4 (đặc biệt nghiêm trọng): sự cố xảy ra đối với các hệ thống đặc biệt quan trọng, làm tê liệt hoạt động của hệ thống hoặc thiệt hại rất nghiêm trọng tới dữ liệu của hệ thống; gây nên những tác động đặc biệt nghiêm trọng cho đơn vị hoặc làm ảnh hưởng lớn tới trật tự xã hội, lợi ích công cộng, đe dọa nghiêm trọng tới an ninh, quốc phòng của đất nước.

Điều 4. Nguyên tắc xử lý sự cố

1. Đảm bảo việc bảo mật thông tin liên quan tới sự cố theo quy định hiện hành của đơn vị và của Bộ Y tế.

2. Việc trao đổi thông tin liên quan tới sự cố có thể được thực hiện bằng nhiều hình thức như thông báo trực tiếp, công văn, thư điện tử, điện thoại, fax. Các cán bộ tiếp nhận thông tin phải chủ động xác thực đối tượng gửi nhằm đảm bảo thông tin gửi đi là tin cậy.

3. Quá trình phát hiện và xử lý sự cố phải được ghi lại trong hồ sơ quản lý sự cố để làm căn cứ theo dõi, báo cáo và rút kinh nghiệm.

4. Yêu cầu về thời gian xử lý sự cố:

a) Đối với sự cố mức 0: Ghi nhận và có phương án xử lý tại thời điểm thích hợp.

b) Đối với sự cố mức 1: Xử lý trong vòng 24h kể từ khi phát hiện hay nhận được thông tin về sự cố.

c) Đối với sự cố mức 2: Xử lý trong vòng 8h kể từ khi phát hiện hay nhận được thông tin về sự cố.

d) Đối với sự cố mức 3: Xử lý trong vòng 4h kể từ khi phát hiện hay nhận được thông tin về sự cố.

đ) Đối với sự cố mức 4: Xử lý ngay lập tức hoặc ngay khi có thể kể từ khi phát hiện hay nhận được thông tin về sự cố.

Chương II
LẬP KẾ HOẠCH XỬ LÝ SỰ CỐ

Điều 5. Kế hoạch xử lý sự cố

1. Các đơn vị cần xây dựng kế hoạch xử lý sự cố cụ thể, chi tiết của đơn vị nhằm cung cấp các thông tin mô tả các quy trình và hoạt động cần thực hiện khi xảy ra sự cố, bao gồm các nội dung cơ bản sau:

a) Xác định, phân loại các hệ thống thông tin của đơn vị;

b) Xem xét, đánh giá các sự kiện có thể phát sinh sự cố đối với các hệ thống thông tin của đơn vị;

c) Đánh giá, phân loại sự cố theo các nguyên tắc phân loại sự cố tại Điều 3 của quy định này;

d) Hướng dẫn các hoạt động cần tiến hành khi phát hiện sự cố và thông báo sự cố theo các nguyên tắc tại Điều 4 của quy định này;

đ) Xây dựng phương án xử lý sự cố đối với từng loại sự cố và tùy theo mức độ nghiêm trọng của sự cố; xác định vai trò của nguồn lực nội bộ cũng như nguồn lực bên ngoài trong quá trình xử lý sự cố; xác định cơ sở vật chất và phương tiện hỗ trợ kỹ thuật sẵn sàng cho hoạt động xử lý sự cố;

e) Hướng dẫn theo dõi sau khi sự cố được xử lý; yêu cầu ghi lại thông tin sự cố cũng như các hoạt động xử lý sự cố vào hồ sơ quản lý sự cố để phục vụ cho việc phân tích sự cố và xác định trách nhiệm của các bên liên quan trong quá trình xử lý sự cố;

g) Yêu cầu báo cáo sự cố định kỳ và khẩn cấp cho lãnh đạo và đơn vị cấp trên;

h) Mẫu báo cáo sự cố và đề xuất các phương án đảm bảo sự cố không xuất hiện trở lại;

i) Xây dựng kế hoạch nâng cao nhận thức và đào tạo về quản lý sự cố cho cán bộ.

2. Kế hoạch xử lý sự cố cần được xem xét và cập nhật trong trường hợp nảy sinh các sự cố mới. Kế hoạch xử lý sự cố và các nội dung cập nhật đều phải được lãnh đạo đơn vị xem xét, phê duyệt.

Điều 6. Cán bộ quản lý sự cố

1. Cán bộ quản lý sự cố là cán bộ thuộc bộ phận chuyên trách công nghệ thông tin của đơn vị. Cán bộ quản lý sự cố có trách nhiệm liên lạc, trao đổi thông tin với các bên liên quan, điều phối các hoạt động xử lý sự cố khi sự cố

xảy ra. Cán bộ quản lý sự cố là đầu mối tiếp nhận phản ánh về sự cố an toàn, an ninh thông tin của đơn vị.

2. Cán bộ quản lý sự cố có trách nhiệm xây dựng kế hoạch xử lý sự cố và điều phối nguồn lực nội bộ hoặc bên ngoài để kịp thời xử lý khi có sự cố xảy ra.

3. Các cán bộ tham gia trong hoạt động xử lý sự cố phải có trình độ chuyên môn và kỹ năng nghiệp vụ phù hợp để thực hiện được công tác xử lý các sự cố liên quan.

4. Đối với các hệ thống đặc biệt quan trọng, cán bộ quản lý sự cố phải đảm bảo khả năng liên lạc thông suốt cho việc xử lý sự cố đối với các hệ thống này (24 giờ trong một ngày và 7 ngày trong tuần).

Điều 7. Các công tác chuẩn bị khác

1. Để đảm bảo sự cố được xử lý một cách nhanh chóng và hiệu quả, cán bộ quản lý sự cố cần chuẩn bị và thường xuyên kiểm tra tất cả các phương tiện hỗ trợ kỹ thuật và các phương tiện cần thiết khác như:

a) Thông tin và tài liệu phục vụ cho việc xử lý sự cố;

b) Các cơ sở dữ liệu dự phòng và các phương tiện sao lưu cơ sở dữ liệu;

c) Trang thiết bị phần cứng, phần mềm, mạng phục vụ cho việc xử lý sự cố.

2. Định kỳ tiến hành kiểm tra các quy trình và thủ tục quản lý sự cố để tìm ra những sai sót tiềm năng và các vấn đề có thể phát sinh.

3. Xây dựng các hoạt động nhằm nâng cao nhận thức cho cán bộ về tầm ảnh hưởng của các sự cố và vai trò của quản lý sự cố. Định kỳ tập huấn về quy trình quản lý sự cố.

Chương III
PHÁT HIỆN VÀ XỬ LÝ SỰ CỐ

Điều 8. Phát hiện và thông báo sự cố

1. Tất cả công chức, viên chức, cán bộ, bên cung cấp dịch vụ công nghệ thông tin và các bên liên quan khi phát hiện các sự cố của đơn vị cần thông báo với cán bộ quản lý sự cố của đơn vị theo những nguyên tắc tại Điều 4 của Quy định này nhằm ngăn chặn các sự cố phát sinh.

2. Nội dung thông báo sự cố bao gồm các nội dung cơ bản sau:

a) Thông tin mô tả sự cố (thời gian xảy ra sự cố, mô tả sự cố);

b) Thông tin liên hệ của tổ chức, cá nhân phát hiện sự cố;

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

3. 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 cán bộ quản lý sự cố của đơn vị và tạo điều kiện thuận lợi cho các cán bộ xử lý sự cố 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 9. Tiếp nhận và xử lý thông báo sự cố

Cán bộ quản lý sự cố sau khi nhận được thông báo về sự cố phải thực hiện các hoạt động sau:

1. Phản hồi cho tổ chức, cá nhân gửi thông báo để xác nhận về việc đã nhận được thông báo sự cố trong vòng 24 giờ kể từ khi nhận được thông báo sự cố.

2. Xác định sự cố là có thật hay là cảnh báo giả.

3. Phân loại sự cố, đánh giá sơ bộ các phần bị ảnh hưởng và tập hợp các thông tin có liên quan đến sự cố.

4. Xác định các cá nhân có trách nhiệm và thông báo về sự cố cũng như các quy trình cần thực hiện cho các cá nhân có liên quan.

5. Ghi nhận lại sự cố vào hồ sơ quản lý sự cố.

6. Báo cáo lãnh đạo trong trường hợp sự cố nghiêm trọng hoặc chưa có kế hoạch xử lý hoặc báo cáo theo các yêu cầu được đưa ra trong kế hoạch xử lý sự cố của đơn vị.

Điều 10. Xử lý sự cố

1. Sau khi tiếp nhận và xử lý thông báo về sự cố, cán bộ quản lý sự cố thực hiện các công việc sau:

a) Phân bổ các nguồn lực nội bộ liên quan tới sự cố và xác định các nguồn lực bên ngoài để ứng phó với mỗi sự cố phát sinh;

b) Công tác xử lý sự cố bao gồm các hoạt động kỹ thuật và các hoạt động khác nhằm xác định nguyên nhân xảy ra sự cố, áp dụng các phương án xử lý sự cố để khôi phục lại hoạt động của hệ thống thông tin, khôi phục lại dữ liệu, đưa hệ thống trở lại hoạt động bình thường. Ghi lại các thông tin xử lý sự cố vào hồ sơ quản lý sự cố của đơn vị. Đối với các sự cố từ mức 3 trở lên, cán bộ quản lý sự cố phải thường xuyên thông báo thông tin về sự cố cho các bên liên quan;

c) Trong trường hợp không xử lý được sự cố, cán bộ xử lý sự cố cần báo cáo trực tiếp lên lãnh đạo đơn vị để lên phương án xử lý bổ sung, đánh giá lại mức độ nghiêm trọng của sự cố, mời thêm các chuyên gia xử lý sự cố, đồng thời

chuẩn bị các thông tin và phương tiện hỗ trợ thích hợp để phối hợp với các bên liên quan xử lý sự cố;

d) Đảm bảo các thông tin về sự cố cũng như các hoạt động xử lý sự cố được ghi lại vào hồ sơ quản lý sự cố để phục vụ cho việc phân tích sự cố và xác định trách nhiệm của các bên liên quan trong quá trình xử lý sự cố.

2. Trong trường hợp các sự cố nghiêm trọng hoặc đặc biệt nghiêm trọng không thể xử lý được, đơn vị cần thực hiện các hoạt động sau:

a) Lãnh đạo đơn vị trực tiếp theo dõi và chỉ đạo quá trình xử lý sự cố;

b) Huy động các nguồn lực bên ngoài, mời chuyên gia tham gia xử lý sự cố;

c) Thông báo cho đơn vị cấp trên và Cục Công nghệ thông tin – Bộ Y tế để hỗ trợ, phối hợp xử lý sự cố nếu cần thiết.

3. Các sự cố đặc biệt nghiêm trọng có ảnh hưởng tới nhiều Bộ, ngành, đã có quy trình xử lý sự cố Quốc gia thì công tác xử lý sự cố cần tuân thủ theo quy trình này.

Chương IV
TỔNG KẾT HOẠT ĐỘNG XỬ LÝ SỰ CỐ VÀ BÁO CÁO CÔNG TÁC QUẢN LÝ SỰ CỐ

Điều 11. Tổng kết hoạt động xử lý sự cố

Sau khi sự cố được xử lý, cán bộ quản lý sự cố cần thực hiện báo cáo tổng kết gửi lãnh đạo đơn vị hoặc báo cáo theo yêu cầu được đưa ra trong kế hoạch quản lý sự cố của đơn vị.

Điều 12. Báo cáo công tác quản lý sự cố

Đối với các sự cố từ mức 3 trở lên, báo cáo tổng kết phải được các đơn vị gửi Cục Công nghệ thông tin – Bộ Y tế để theo dõi, cập nhật vào cơ sở dữ liệu sự cố. Báo cáo bao gồm các nội dung sau:

1. Phân tích nguyên nhân, thực trạng và biện pháp đã sử dụng để xử lý sự cố.

2. Thông báo các điểm yếu trong hệ thống thông tin và phương án xử lý để hạn chế việc xảy ra sự cố tương tự.

3. Thông báo các điểm chưa phù hợp trong quy trình quản lý sự cố và kế hoạch xử lý sự cố đã có.

4. Rà soát và bổ sung, cập nhật các sự cố, nguy cơ mất an toàn thông tin có thể xảy ra.

5. Rà soát, bổ sung, cập nhật quy trình quản lý sự cố và kế hoạch xử lý sự cố cho phù hợp.

Chương V
TRÁCH NHIỆM CỦA CÁC TỔ CHỨC, CÁ NHÂN

Điều 13. Trách nhiệm của các đơn vị trong ngành y tế

1. Cử cán bộ quản lý sự cố và bảo đảm cán bộ quản lý sự cố tuân thủ đúng Điều 6 của Quy định này.

2. Xây dựng và phê duyệt kế hoạch quản lý sự cố theo Điều 5 của Quy định này.

3. Tiếp nhận và xử lý các thông báo sự cố theo Điều 9 của Quy định này.

4. Xử lý sự cố theo Điều 10 của Quy định này.

5. Phối hợp, hỗ trợ các đơn vị khác trong các hoạt động ứng cứu sự cố.

6. Ghi nhận thông tin sự cố và thông tin xử lý sự cố vào hồ sơ quản lý sự cố, 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 và thời gian nhận được xác nhận đối với trường hợp thông báo cho đơn vị cấp trên hoặc Cục Công nghệ thông tin.

7. Ưu tiên bố trí kinh phí và cơ sở vật chất, phương tiện kỹ thuật ứng phó sự cố.

Điều 14. Trách nhiệm của Cục Công nghệ thông tin – Bộ Y tế

1. Xây dựng, cập nhật các quy định, hướng dẫn cụ thể về quản lý sự cố trong ngành y tế.

2. Cử đầu mối tiếp nhận, hỗ trợ các đơn vị xử lý các sự cố do các đơn vị gửi đến.

3. Tổng hợp và thông báo thông tin về các sự cố đặc biệt nghiêm trọng cho các đơn vị trong ngành y tế, đưa ra cảnh bảo về các sự cố có nguy cơ cao xảy ra.

4. Xây dựng, cập nhật cơ sở dữ liệu sự cố thuộc Bộ Y tế. Chia sẻ thông tin về các phương án xử lý sự cố cho các các đơn vị trong ngành nghiên cứu, học tập.

5. Xây dựng chương trình đào tạo và tổ chức đào tạo, tập huấn công tác quản lý sự cố.

Chương VI
TỔ CHỨC THỰC HIỆN

Điều 15. Hiệu lực thi hành

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

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 Y tế (Cục Công nghệ thông tin) để xem xét, bổ sung và sửa đổi./.

KT.BỘ TRƯỞNG
THỨ TRƯỞNG

Lê Quang Cường

PHỤ LỤC 01
MẪU THÔNG BÁO SỰ CỐ AN TOÀN THÔNG TIN

1. Thông tin về cá nhân / tổ chức thông báo sự cố

Tên: .....

Đơn vị: .....

Email: .....

Điện thoại: .....

2. Thông tin về sự cố

2.1. Địa điểm xảy ra sự cố: .....

2.2. 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)

2.3. Thời gian thông báo sự cố: …./…./…./…./…. (ngày/tháng/năm/giờ/phút)

2.4. Mô tả sơ bộ về sự cố: .....

2.5. Cách thức phát hiện sự cố: .....

2.6. Đã gửi thông báo sự cố cho:

☐ Lãnh đạo đơn vị xảy ra sự cố (nêu rõ cá nhân nếu có thể): .....

bằng hình thức: ☐ Thông báo trực tiếp ☐ Email

☐ Gửi thư/công văn ☐ Gọi điện thoại

☐ Đầu mối xử lý sự cố (nêu rõ cá nhân nếu có thể): .....

bằng hình thức: ☐ Thông báo trực tiếp ☐ Email

☐ Gửi thư/công văn ☐ Gọi điện thoại

☐ Đơn vị cung cấp dịch vụ (nêu rõ nếu có thể): .....

bằng hình thức: ☐ Thông báo trực tiếp ☐ Email

☐ Gửi thư/công văn ☐ Gọi điện thoại

☐ Khác:.....

bằng hình thức: ☐ Thông báo trực tiếp ☐ Email

☐ Gửi thư/công văn ☐ Gọi điện thoại

2.7. Thông tin chi tiết về hệ thống xảy ra sự cố: .....

2.8. Thông tin gửi kèm: .....

2.9. Yêu cầu giữ bí mật các thông tin cung cấp trên đây:

☐ Có ☐ Không

3. Kiến nghị

.....

.....

.....

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

Cá nhân / đại diện tổ chức thông báo

(ký và ghi rõ họ tên)

PHỤ LỤC 02
HỒ SƠ QUẢN LÝ SỰ CỐ

1. Thông tin về sự cố

1.1. Họ tên người thông báo sự cố:.....

1.2. Chức vụ:.....

1.3. Địa điểm xảy ra sự cố:.....

1.4. 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)

1.5. Thời gian thông báo sự cố: …./…./…./…./…. (ngày/tháng/năm/giờ/phút)

1.6. Thời gian thông báo Cục Công nghệ thông tin – Bộ Y tế: …./…./…./…./…. (ngày/tháng/năm/giờ/phút)

1.7. Cách thức phát hiện sự cố:.....

1.8. Số sự cố:.....

1.9. Loại sự cố: .....

1.10. Mức độ sự cố: .....

2. Nội dung tiếp nhận sự cố

2.1. Mô tả sự cố: .....

.....

2.2. Nguyên nhân sơ bộ gây ra sự cố:.....

.....

2.3. Nhật ký xử lý sự cố:.....

.....

3. Nội dung xử lý sự cố

3.1. Kết quả xử lý sự cố:.....

.....

3.2. Tổ chức, cá nhân xử lý sự cố:.....

.....

3.3. Bài học kinh nghiệm:.....

.....

PHỤ LỤC 03
MẪU BÁO CÁO SỰ CỐ AN TOÀN THÔNG TIN

Thời gian: từ ngày.....tháng.....năm.....đến ngày.....tháng.....năm.....

1. Thông tin về đơn vị/tổ chức

1.1. Tên đơn vị: .....

1.2. Địa chỉ: .....

2. Mô tả hệ thống

2.1. Chức năng của hệ thống: .....

2.2. Tầm quan trọng của hệ thống : .....

2.3. Các dịch vụ có trên hệ thống: .....

2.4. Các biện pháp đảm bảo an toàn thông tin đã triển khai: .....

3. Thông tin về sự cố và cách thức xử lý

3.1. Mô tả sự cố: .....

3.2. Mức độ sự cố: .....

3.3. Nguyên nhân sự cố: .....

.....

3.4. Phương án xử lý sự cố: .....

.....

3.5. Thời gian xử lý sự cố: .....

3.6. Tổ chức, cá nhân tham gia xử lý sự cố: .....

4. Đề xuất kiến nghị:

.....

.....

.....

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

Lãnh đạo đơn vị

(đóng dấu, ký và ghi rõ họ tên)

PHỤ LỤC 04
VÍ DỤ MỘT SỐ SỰ CỐ AN TOÀN THÔNG TIN

Loại sự cố	Mô tả
Sự cố do lây nhiễm phần mềm độc hại	Mất an toàn thông tin do lây nhiễm phần mềm độc hại. Phần mềm độc hại được cài đặt bí mật vào hệ thống nhằm gây tổn hại đến tính bí mật, toàn vẹn, sẵn sàng của dữ liệu, ứng dụng hoặc ảnh hưởng đến hoạt động của hệ thống. Ví dụ lây nhiễm vi rút máy tính, mã độc…
Sự cố do tấn công kỹ thuật	Mất an toàn thông tin do bị tấn công bằng kỹ thuật, công nghệ vào các điểm yếu của hệ thống dẫn đến ngừng hoạt động của hệ thống, cản trở các hoạt động dịch vụ của đơn vị. Ví dụ như tấn công từ chối dịch vụ DDOS, chiếm quyền điều khiển hệ thống thông qua khai thác cổng sau BACKDOOR…
Sự cố do vi phạm quy định	Sự cố do lỗi cố ý vi phạm của con người ví dụ như xâm nhập vào khu vực không đươc phép, vi phạm bản quyền…
Sự cố mất mát thông tin, dữ liệu	Mất an toàn thông tin do cố tính hoặc vô ý làm mất mát thông tin, dữ liệu, ảnh hưởng tới tính bảo mật, tính toàn vẹn, tính sẵn sàng của thông tin như trộm cắp, giả mạo thông tin, dữ liệu…
Sự cố do thiên tai	Các sự cố do thiên thai gây ra như động đất, lũ lụt…
Sự cố do lỗi cơ sở hạ tầng	Các sự cố do lỗi cơ sở hạ tầng như mất điện, lỗi mạng, sự cố điều hòa không khí…