CỤC BẢO TỒN THIÊN NHIÊN
VÀ ĐA DẠNG SINH HỌC
TRUNG TÂM ĐIỀU TRA, THÔNG TIN VÀ DỮ LIỆU VỀ MÔI TRƯỜNG, ĐA DẠNG SINH HỌC

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

Hà Nội, ngày 28 tháng 5 năm 2024

Số: 86 /QĐ-ĐTTTDL

QUYẾT ĐỊNH
Về việc ban hành Quy trình xử lý sự cố an toàn, an ninh thông tin

GIÁM ĐỐC TRUNG TÂM ĐIỀU TRA, THÔNG TIN VÀ DỮ LIỆU VỀ MÔI TRƯỜNG, ĐA DẠNG SINH HỌC

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Luật An ninh mạng ngày 12 tháng 6 năm 2018;

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 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 của 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 Thông tư số 14/2020/TT-BTNMT ngày 27 tháng 11 năm 2020 của Bộ Tài nguyên và Môi trường quy định quy trình và định mức kinh tế - kỹ thuật kỹ xây dựng, duy trì, vận hành hệ thống thông tin ngành tài nguyên và môi trường;

Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 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 Quyết định số 187/QĐ-BTĐD ngày 04 tháng 10 năm 2023 của Cục trưởng Cục Bảo tồn thiên nhiên và Đa dạng sinh học về việc ban hành Quy chế bảo đảm an toàn, an ninh thông tin mạng Cục Bảo tồn thiên nhiên và Đa dạng sinh học;

Căn cứ Quyết định số 3856/QĐ-BTNMT ngày 30 tháng 12 năm 2022 của Bộ Tài nguyên và Môi trường quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Trung tâm Điều tra, Thông tin và Dữ liệu về môi trường, đa dạng sinh học trực thuộc Cục Bảo tồn thiên nhiên và Đa dạng sinh học;

Theo đề nghị của Trưởng phòng Quản trị hệ thống thông tin môi trường, đa dạng sinh học,

QUYẾT ĐỊNH

Điều 1. Ban hành kèm theo Quyết định này Quy trình xử lý các sự cố an toàn, an ninh thông tin.

Điều 2. Quyết định này có hiệu lực từ ngày ký và làm căn cứ để triển khai thực hiện.

Điều 3. Chánh Văn phòng, Trưởng các phòng chuyên môi thuộc Trung tâm, viên chức, người lao động của Trung tâm Điều tra, Thông tin và Dữ liệu về môi trường, đa dạng sinh học và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Cục trưởng Nguyễn Văn Tài (để báo cáo);
- Các Phó Cục trưởng (để báo cáo);
- Các đơn vị trực thuộc Cục BTĐD (để phối hợp);
- Các Phòng trực thuộc Trung tâm (để thực hiện);
- Lưu: VT, ĐTTTDL, HA06.

GIÁM ĐỐC

BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TRUNG TÂM ĐIỀU TRA, THÔNG TIN VÀ DỮ LIỆU VỀ MÔI TRƯỜNG, ĐA DẠNG SINH HỌC
CỤC BẢO TỒN THIÊN NHIÊN VÀ ĐA DẠNG SINH HỌC

Nguyễn Văn Thùy

QUY TRÌNH
XỬ LÝ CÁC SỰ CỐ AN TOÀN, AN NINH THÔNG TIN

(Ban hành kèm theo Quyết định số 86 /ĐTTTDL ngày 28 tháng 5 năm 2024 của Trung tâm Điều tra, Thông tin và Dữ liệu về môi trường, đa dạng sinh học)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quyết định này ban hành Quy trình quản lý, xử lý sự cố an toàn thông tin 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 trong công tác giám sát và cảnh báo an toàn thông tin.

2. Quy trình này áp dụng đối với các đơn vị, tổ chức triển khai ứng dụng công nghệ thông tin trong việc 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:* là sự kiện đã, đang, hoặc có khả năng xảy ra gây mất an toàn, an ninh thông tin 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 (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 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 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 có ảnh hưởng đáng kể tới an ninh, xã hội 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 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.

Chương II
PHÂN TÍCH VÀ THÔNG BÁO SỰ CỐ

Điều 3. Tiếp nhận, xác định sự cố

Phòng Quản trị hệ thống thông tin môi trường, đa dạng sinh học (gọi tắt là P.QTHT) là phòng quản trị, vận hành và duy trì các hệ thống thông tin của Trung tâm chịu trách nhiệm chủ trì, phối hợp các cơ quan, tổ chức liên quan tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài, tất cả 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 (cảnh báo sự cố: Công văn, email, điện thoại, website, facebook, mạng xã hội,...; phát hiện sự cố thông qua kiểm tra, rà soát, đánh giá). Khi xác định được sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp, gồm:

a) Sự cố do bị tấn công mạng.

b) Sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật hoặc do lỗi đường điện, đường truyền, hosting...

c) Sự cố do lỗi của người quản trị, vận hành hệ thống.

d) Sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn,...

Điều 4. Triển khai các bước ưu tiên ứng cứu ban đầu

Sau khi đã xác định sự cố xảy ra, P. QTHT triển khai các bước ưu tiên ban đầu để xử lý sự cố theo phương án, kế hoạch ứng phó sự cố đã được cấp thẩm quyền phê duyệt/xác nhận hoặc theo tư vấn, hướng dẫn của Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường (các bước thực hiện chi tiết tại phụ lục 01 kèm theo).

Điều 5. 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, ứng dụng triển khai trong ngành.

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.

f) 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.

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

h) 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 6. Thông báo, báo cáo sự cố

Sau khi triển khai các bước ưu tiên ứng cứu ban đầu, P.QTHT tổ chức thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan, tổ chức theo quy định. Cụ thể:

a) Thông báo sự cố tới Lãnh đạo Trung tâm khi phát hiện sự cố; trường hợp xác định sự cố có thể vượt khả năng xử lý, P.QTHT phải báo cáo ban đầu sự cố bằng văn bản về Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường.

b) Hình thức thông báo sự cố: bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện, phần mềm gửi nhận văn bản, phần mềm điều hành tác nghiệp.

c) Hình thức báo cáo sự cố: bằng văn bản giấy hoặc văn bản điện tử.

Điều 7. 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 Tài nguyên và Môi trường.

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 III
LẬP KẾ HOẠCH XỬ LÝ SỰ CỐ

Điều 8. Kế hoạch xử lý sự cố

1. P.QTHT xây dựng kế hoạch xử lý sự cố 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 5 của quy chế 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 6 của quy chế 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.

f) Yêu cầu báo cáo sự cố định kỳ và khẩn cấp cho Lãnh đạo và đơn vị cấp trên.

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

h) 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 phát 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. Báo cáo phân tích và đề xuất giải pháp khắc phục sự cố chi tiết tại phụ lục 02 gửi kèm.

Điều 9. Cán bộ quản lý sự cố

1. Cán bộ quản lý sự cố là cán bộ thuộc P.QTHT 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 10. 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.

Điều 11. 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 tại phụ lục 03 kèm theo. 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 Lãnh đạo Trung tâm và Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường 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 hướng dẫn của Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường.

Chương IV

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

Điều 12. 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 Trung tâm hoặc báo cáo theo yêu cầu được đưa ra trong kế hoạch quản lý sự cố của đơn vị.

Điều 13. Báo cáo công tác quản lý sự cố

Đối với các sự cố từ mức 3 trở lên, báo cáo tổng kết phải được gửi Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường 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 VÀ TỔ CHỨC THỰC HIỆN

Điều 14. Trách nhiệm của phòng Quản trị hệ thống quản trị hệ thống thông tin môi trường, đa dạng sinh học

1. Đầu mối, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố an toàn thông tin của các hệ thống thông tin do Trung tâm quản lý, vận hành.

2. 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.

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

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

5. Xử lý sự cố theo Điều 11 của Quy chế này.

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

7. 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). Bản thống kê danh mục sự cố chi tiết tại phụ lục 04.

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 Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường.

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

Điều 15. Trách nhiệm của các phòng thuộc Trung tâm

1. Phối hợp với P.QTHT trong quá trình ứng cứu sự cố an toàn thông tin khi xảy ra sự cố.

2. Các viên chức, người lao động của các phòng có trách nhiệm: tuân thủ nghiêm các quy định về bảo đảm an toàn, an ninh thông tin mạng; thông báo kịp thời các vấn đề bất thường liên quan tới an toàn thông tin cho P.QTHT khi phát hiện sự cố an toàn thông tin.

Điều 16. Tổ chức thực hiện

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

2. Trong quá trình thực hiện, nếu có vướng mắc, phát sinh tổ chức, cá nhân có liên quan kịp thời phản ánh về Phòng Quản trị hệ thống thông tin môi trường, đa dạng sinh học để trình Lãnh đạo xem xét, bổ sung và sửa đổi cho phù hợp./.

PHỤ LỤC
QUY TRÌNH ỨNG CỨU SỰ CỐ AN TOÀN, AN NINH THÔNG TIN

(Ban hành kèm Quyết định số /QĐ-ĐTTTDL ngày tháng năm 2024 của Trung tâm Điều tra, Thông tin và Dữ liệu về môi trường, đa dạng sinh học)

PHỤ LỤC 01
CÁC BƯỚC TRONG QUY TRÌNH XỬ LÝ SỰ CỐ AN TOÀN, AN NINH THÔNG TIN

1. Lược đồ quy trình ứng cứu, xử lý sự cố an toàn , an ninh thông tin

2. Mô tả các bước trong quy trình ứng cứu, xử lý sự cố an toàn, an ninh thông tin

Hệ thống thông tin phải thường xuyên rà quét và thực hiện cấu hình hệ thống, thiết bị để lưu nhật lý (log), giám sát hệ thống.

2.1. Phát hiện, báo cáo sự cố

a) Bộ phận chủ trì: Phòng Quản trị hệ thống thông tin môi trường, đa dạng sinh học (P.QTHT).

b) Bộ phận phối hợp: Cục Chuyển đổi số và Thông tin dữ liệu tài nguyên môi trường (Cục CĐS&TTDLTNMT)

c) Nội dung công việc:

P.QTHT phối hợp với Cục CĐS&TTDLTNMT và các đơn vị liên quan tiến hành:

Bước 1: Đối với sự cố tự phát hiện được, thực hiện:

- Thu thập thông tin, log: dấu hiệu sự cố, thu thập log (ứng dụng, thiết bị mạng, thiết bị bảo mật,…) phục vụ xác định nguyên nhân, nguồn gốc sự cố, từ đó phân loại sự cố:

+ Sự cố về tấn công từ chối dịch vụ;

+ Sự cố về tấn công giả mạo;

+ Sự cố về tấn công sử dụng mã độc;

+ Sự cố về tấn công truy cập trái phép, chiếm quyền điều khiển;

+ Sự cố về tấn công thay đổi giao diện;

+ Sự cố về tấn công mã hóa phần mềm, dữ liệu, thiết bị;

+ Sự cố về tấn công phá hoại thông tin, dữ liệu, phần mềm;

+ Sự cố về tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu;

+ Sự cố về tấn công tổng hợp sử dụng kết hợp nhiều hình thức;

+ Sự cố về các hình thức tấn công mạng khác.

- Báo cáo tình hình cho chủ quản hệ thống thông tin và Lãnh đạo Trung tâm để chỉ đạo xử lý và phân công trách nhiệm xử lý.

- Báo cáo sự cố chi tiết về Cục CĐS&TTDLTNMT (*Mẫu báo cáo phân tích và đề xuất giải pháp khắc phục sự cố phụ lục 02 kèm theo*)

- Thực hiện các tác vụ khác theo quy trình ứng cứu sự cố nội bộ.

Bước 2: Đối với sự cố do Cục CĐS&TTDLTNMT cảnh báo:

- Gửi xác nhận đã nhận được cảnh báo về Cục CĐS&TTDLTNMT.

- Cử đầu mối phối hợp (họ tên, chức vụ, phòng ban, số di động, email).

- Thực hiện các hoạt động như nội dung tại (Bước 1).

d) Thời gian thực hiện: Tối đa 06 giờ.

2.2. Xác định hình thức tấn công, mức độ khẩn cấp

a) Bộ phận chủ trì: P.QTHT

b) Bộ phận phối hợp: Cục CĐS&TTDLTNMT.

c) Nội dung công việc:

P.QTHT phối hợp với Cục CĐS&TTDLTNMT tiến hành thu thập thông tin để phân tích sự cố:

+ Thông tin về đầu mối liên hệ;

+ Thu thập thông tin hệ thống;

+ Thu thập chức năng của hệ thống;

+ Thu thập cấu hình của hệ thống (OS, Servise, version, network...);

+ Thu thập chứng cứ;

+ Thu thập bộ nhớ;

+ Thu thập trạng thái network và các kết nối;

+ Thu thập các tiến trình đang chạy;

+ Thu thập hard drive media;

+ Thu thập log file;

+ Thu thập các cổng đang mở của hệ thống.

Bước 1: Trường hợp bộ phận ứng cứu tự phân tích, xử lý được:

- Kiểm tra, theo dõi nội dung trên hệ thống, website; kiểm tra log (ứng dụng, thiết bị mạng, thiết bị bảo mật,…).

- Theo dõi, đánh giá lưu lượng trên hệ thống giám sát, trên log để đánh giá tình hình, phát hiện sự cố bất thường.

- Rà soát, kiểm tra dấu hiệu bất thường của dữ liệu, cấu hình, tài khoản trên hệ thống.

- Trên cơ sở đó xác định hình thức tấn công và mức độ khẩn cấp của sự cố.

- Sao lưu dữ liệu phục vụ xác minh, truy vết sự cố. Trong trường hợp thiết, thực hiện cô lập hệ thống.

- Thực hiện các nội dung khác theo quy trình nội bộ.

Bước 2: Trường hợp P.QTHT không tự phân tích, xử lý được:

- Liên hệ ngay với Cục CĐS&TTDLTNMT để được hỗ trợ phân tích.

- Cung cấp đầy đủ các thông tin về sự cố theo yêu cầu của Cục CĐS&TTDLTNMT.

d) Thời gian thực hiện: tối đa 03 giờ.

2.3. Ứng cứu sự cố, khôi phục hệ thống

a) Bộ phận chủ trì: P.QTHT.

b) Bộ phận phối hợp: Cục CĐS&TTDLTNMT.

c) Nội dung công việc:

P.QTHT tiếp tục phối hợp với Cục CĐS&TTDLTNMT tiến hành phân tích sự cố và xử lý sự cố:

- Phân tích sự cố:

+ Phân tích dòng thời gian;

+ Thời gian bị sửa đổi, truy cập, tạo hoặc thay đổi.

+ Thời gian thực hiện các cập nhật lớn đối với hệ thống;

+ Thời điểm mà hệ thống sử dụng lần cuối cùng;

+ Phân tích dữ liệu ...

- Xử lý sự cố:

+ Gỡ bỏ sự cố;

+ Xác định và gỡ bỏ các backdoors;

+ Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi;

+ Khôi phục;

+ Phân tích và kiểm tra lỗ hổng sau khi thực hiện các bản vá lỗi;

+ Khôi phục dữ liệu;

+ Thu thập các tệp tin, hình ảnh, email,... bị xóa, thời gian bị xóa;

+ Tìm kiếm các tệp tin không thể khôi phục;

+ Khôi phục các tệp tin phù hợp.

Bước 1: Trường hợp tiếp tục tự xử lý được:

- Căn cứ vào sự cố và hình thức tấn công thực hiện cấu hình các hệ thống để chặn lọc các nguồn tấn công, giảm thiểu tác động của cuộc tấn công và khôi phục lại hệ thống:

- Đề nghị các nhà cung cấp dịch vụ vận hành, an toàn thông tin,… có liên quan hỗ trợ các công cụ, giải pháp, thiết bị, nhân sự tham gia ứng cứu sự cố;

- Yêu cầu nhà cung cấp dịch vụ hỗ trợ điều hướng, chặn/lọc nguồn tấn công, tăng băng thông, tài nguyên tạm thời;

- Thực hiện các nội dung khác theo quy trình nội bộ.

Bước 2: Trường hợp không tiếp tục tự xử lý được:

- Liên hệ ngay với Cục CĐS&TTDLTNMT để được hỗ trợ phân tích, đánh giá tình trạng;

- Cung cấp đầy đủ các thông tin về sự cố theo yêu cầu của Cục CĐS&TTDLTNMT.

d) Thời gian thực hiện: Tối đa 09 giờ.

2.4. Điều phối ứng cứu sự cố

Trong trường hợp cần thiết, Cục CĐS&TTDLTNMT thực hiện điều phối ứng cứu sự cố.

a) Bộ phận chủ trì: Cục CĐS&TTDLTNMT

b) Bộ phận phối hợp: Bộ phận ứng cứu sự cố của Bộ, P.QTHT.

c) Nội dung công việc:

Căn cứ trên tình hình thực tế, Cục CĐS&TTDLTNMT sẽ:

- Điều phối lực lượng kỹ thuật của Cục CĐS&TTDLTNMT để hướng dẫn các tác nghiệp ứng cứu, xử lý sự cố, khôi phục hệ thống từ xa hoặc thực hiện ứng cứu, xử lý sự cố, khôi phục hệ thống ngay tại hiện trường;

- Điều phối các đơn vị chuyên trách về ứng cứu sự cố có liên quan thực hiện ứng cứu khẩn cấp sự cố;

- Điều phối P.QTHT, doanh nghiệp/tổ chức cung cấp dịch vụ cung cấp thông tin, thực hiện các tác nghiệp ứng cứu, xử lý sự cố và khôi phục hệ thống, phân tích, xác minh, truy vết sự cố (nếu cần);

- Hướng dẫn khắc phục, phòng ngừa sự cố tái diễn.

d) Thời gian thực hiện: Tối đa 09 giờ.

2.5. Kết thúc xử lý sự cố

a) Bộ phận chủ trì: P.QTHT.

b) Bộ phận phối hợp: Cục CĐS&TTDLTNMT

c) Nội dung công việc:

- Thực hiện các nghiệp vụ nhằm phân tích xác minh chuyên sâu về sự cố;

- Gửi báo cáo kết thúc sự cố về cho Cục CĐS&TTDLTNMT qua email. Báo cáo gồm các thông tin: Diễn biến sự cố, cách thức xử lý sự cố và thời gian xử lý xong sự cố (*Mẫu báo cáo khắc phục sự cố phụ lục 02 kèm theo*).

- Thực hiện các tác vụ khác theo quy trình ứng cứu sự cố.

d) THời gian thực hiện: Tối đa 06 giờ.

2.6. Khắc phục, phòng ngừa sự cố tái diễn.

a) Bộ phận chủ trì: P.QTHT.

b) Bộ phận phối hợp: Cục CĐS&TTDLTNMT

c) Nội dung công việc:

- Triển khai các biện pháp khắc phục lỗ hổng, điểm yếu;

- Tăng cường giải pháp bảo vệ, phòng ngừa;

- Rà soát quy trình ứng cứu, khắc phục các điểm yếu trong quy trình.

d) Thời gian thực hiện: Do đơn vị chủ quản.

2.7. Hỗ trợ sau sự cố

a) Bộ phận chủ trì: Cục CĐS&TTDLTNMT

b) Bộ phận phối hợp: P.QTHT

c) Nội dung công việc:

- Tiếp tục theo dõi kết quả, hỗ trợ khắc phục sự cố trong thời gian tiếp theo;

- Khuyến nghị các biện pháp bảo đảm an toàn, an ninh mạng cần triển khai để khắc phục các lỗ hổng dẫn đến sự cố.

d) Thời gian thực hiện: Trong vòng 01 tuần sau khi kết thúc xử lý sự cố.

PHỤ LỤC 02

BÁO CÁO PHÂN TÍCH VÀ ĐỀ XUẤT GIẢI PHÁP KHẮC PHỤC SỰ CỐ

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

BÁO CÁO PHÂN TÍCH VÀ ĐỀ XUẤT GIẢI PHÁP KHẮC PHỤC SỰ CỐ

Kính gửi:……

- Phòng: .....
- Người lập báo cáo ..... Chức vụ:.....
- Điện thoại (*) ..... Email (*) .....

I. THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên sự cố:	
Tên thiết bị, hệ thống gặp sự cố	
Cán bộ vận hành giám sát:	
Cán bộ hệ thống xử lý sự cố:	

Mô tả sơ bộ về sự cố (*)
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ sự cố đã xảy ra và phương án thực hiện.: ....

Ngày phát hiện sự cố (*) (dd/mm/yy)	/ /	Thời gian phát hiện (*):	…..giờ…. phút

CÁCH THỨC PHÁT HIỆN

☐ Qua phần mềm, hệ thống ☐ Kiểm tra dữ liệu lưu lại (Log File)

☐ Nhận được thông báo từ: .....

☐ Khác, đó là .....

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

☐ Các phòng, ban đang sử dụng các dịch vụ trên hệ thống
☐ Nhà cung cấp dịch vụ, đơn vị cung cấp thiết bị
☐ Lãnh đạo đơn vị

II. PHÂN TÍCH SỰ CỐ

Phân tích các nguyên nhân gây ra sự cố (*)
Đề nghị phân tích các nguyên nhân, yếu tố gây ra sự cố hoặc có tác động trực tiếp đến sự cố.:.....

III. ĐỀ XUẤT CÁC GIẢI PHÁP KHẮC PHỤC SỰ CỐ

Các giải pháp khắc phục sự cố (*)
Đề nghị cung cấp các giải pháp có thể thực hiện để khắc phục sự cố và những tác động tới hệ thống khi thực hiện các giải pháp đó.: ..... Giải pháp 1: ..... - Các bước thực hiện: - Các nguy cơ, ảnh hưởng khi thực hiện giải pháp này trên hệ thống - Cảnh báo: .... Giải pháp 2: ..... - Các bước thực hiện: - Các nguy cơ, ảnh hưởng khi thực hiện giải pháp này trên hệ thống - Cảnh báo: .... Giải pháp 3: ..... - Các bước thực hiện:

- Các nguy cơ, ảnh hưởng khi thực hiện giải pháp này trên hệ thống
- Cảnh báo: .....

.....
.....
.....
.....

NGƯỜI LẬP BÁO CÁO
(Ký và ghi rõ họ tên)

LÃNH ĐẠO ĐƠN VỊ
(ký, ghi rõ họ tên và đóng dấu)

PHỤ LỤC 03

BÁO CÁO KHẮC PHỤC SỰ CỐ DUY TRÌ VẬN HÀNH HỆ THỐNG CÔNG NGHỆ THÔNG TIN

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

BÁO CÁO KHẮC PHỤC SỰ CỐ
DUY TRÌ VẬN HÀNH HỆ THỐNG CÔNG NGHỆ THÔNG TIN

Kính gửi: ……..

- Phòng: .....
- Người lập báo cáo ..... Chức vụ: .....
- Điện thoại (*) .....Email (*).....

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên sự cố:	
Tên thiết bị, hệ thống gặp sự cố	
Cán bộ vận hành giám sát:	
Cán bộ hệ thống xử lý sự cố:	

Mô tả sơ bộ về sự cố (*)
Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ sự cố đã xảy ra và phương án thực hiện.: ....

Ngày phát hiện sự cố (*) (dd/mm/yy)	/ /	Thời gian phát hiện (*):	…..giờ…. phút

HIỆN TRẠNG SỰ CỐ (*)

☐ Đã được xử lý ☐ Chưa được xử lý

CÁCH THỨC PHÁT HIỆN

☐ Qua phần mềm, hệ thống ☐ Kiểm tra dữ liệu lưu lại (Log File)

☐ Nhận được thông báo từ: .....

☐ Khác, đó là .....

ĐÃ GỬI THÔNG BÁO SỰ CỐ CHO *

☐ Các phòng, ban đang sử dụng các dịch vụ trên hệ thống

☐ Nhà cung cấp dịch vụ, đơn vị cung cấp thiết bị

☐ Lãnh đạo đơn vị

THÔNG TIN BỔ SUNG VỀ HỆ THỐNG XẢY RA SỰ CỐ

- Tên phần cứng bị 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

  .....
- Các tên miền của hệ thống

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

  .....
- Thông tin gửi kèm

☐ Nhật ký xử lý sự cố ☐ 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 hỗ trợ từ đơn vị ngoài)
- Kiến nghị .....

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ *: …/… /……/…/…

(ngày/tháng/năm/giờ/phút)

Người lập báo cáo

(Ký tên)

PHỤ LỤC 04
BẢNG DANH MỤC SỰ CỐ

HƯỚNG DẪN QUY ĐỊNH THỰC HIỆN:

1. Mục đích: Ghi chép lại các sự cố đã xảy ra trong quá trình duy trì, vận hành các hệ thống, dịch vụ công nghệ thông tin và phần mềm, cơ sở dữ liệu ngành Tài nguyên và môi trường

2. Cách ghi nhật ký:

a) Ghi lại sự cố gặp phải trong quá trình vận hành hệ thống;

b) Ghi lại các giải pháp đã triển khai để khắc phục sự cố.

STT	Ngày	Tên sự cố	Mô tả chi tiết sự cố	Phân nhóm sự cố					Giải pháp khắc phục đã thực hiện	Cán bộ xử lý
				Phần mềm	CSDL	Phần cứng CNTT	Dịch vụ mạng	Tổng hợp		
1										
2										
3										
…										