BẢO HIỂM XÃ HỘI VIỆT NAM	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1603 /QĐ-BHXH	*Hà Nội, ngày* 09 *tháng* 09 *năm 2024*

QUYẾT ĐỊNH
Quy trình ứng cứu sự cố an toàn thông tin mạng ngành Bảo hiểm xã hội Việt Nam

TỔNG GIÁM ĐỐC BẢO HIỂM XÃ HỘI VIỆT NAM

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 Nghị định 89/2020/NĐ-CP, ngày 04 tháng 8 năm 2020 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bảo hiểm xã hội Việt Nam;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ 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 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 Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 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 957/QĐ-BHXH ngày 05 tháng 7 năm2024 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam về việc kiện toàn ban chỉ đạo chuyển đổi số ngành Bảo hiểm xã hội;

Căn cứ Quyết định số 987/QĐ-BHXH ngày 11 tháng 7 năm 2024 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam kiện toàn đội ứng cứu sự cố an toàn thông tin mạng ngành Bảo hiểm xã hội Việt Nam;

Căn cứ Quyết định số 1738/QĐ-BHXH ngày 29 tháng 11 năm 2021 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam ban hành Quy chế hoạt động Ban chỉ đạo và Tổ giúp việc Ban chỉ đạo Chuyển đổi số ngành Bảo hiểm xã hội Việt Nam;

Căn cứ Kế hoạch số 3280/KH-BHXH ngày 29 tháng 8 năm 2018 của Bảo hiểm xã hội Việt Nam ứng phó sự cố bảo đảm an toàn thông tin mạng trong ngành Bảo hiểm xã hội Việt Nam;

Căn cứ Quyết định số 2358/QĐ-BHXH ngày 19 tháng 9 năm 2022 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam phê duyệt kiến trúc Chính phủ điện tử ngành Bảo hiểm xã hội Việt Nam, phiên bản 2.0;

Theo đề nghị của Giám đốc Trung tâm Công nghệ thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này "Quy trình ứng cứu sự cố an toàn thông tin mạng ngành Bảo hiểm xã hội Việt Nam".

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

Điều 3. Giám đốc Trung tâm Công nghệ thông tin, Chánh Văn phòng Bảo hiểm xã hội Việt Nam, Thủ trưởng các đơn vị trực thuộc Bảo hiểm xã hội Việt Nam, Giám đốc Bảo hiểm xã hội các tỉnh, thành phố trực thuộc Trung ương và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như điều 3;
- Tổng Giám đốc;
- Các Phó Tổng Giám đốc;
- Lưu: VT, CNTT.

TỔNG GIÁM ĐỐC

BẢO HIỂM XÃ HỘI VIỆT NAM

Nguyễn Thế Mạnh

BẢO HIỂM XÃ HỘI VIỆT NAM

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

Hà Nội, ngày tháng năm 2024

QUY TRÌNH
Ứng cứu sự cố an toàn thông tin mạng ngành Bảo hiểm xã hội Việt Nam

(*Ban hành kèm theo Quyết định số /QĐ-BHXH ngày tháng năm 2024 của Tổng Giám đốc Bảo hiểm xã hội Việt Nam*)

I. QUY ĐỊNH CHUNG

1. Phạm vi điều chỉnh

Quy trình này quy định trình tự và hướng dẫn thực hiện hoạt động ứng cứu sự cố an toàn thông tin mạng trong ngành Bảo hiểm xã hội Việt Nam.

2. Đối tượng áp dụng

a) Công chức, viên chức và người lao động tham gia quản lý, vận hành, duy trì, phát triển và bảo đảm an toàn thông tin mạng phục vụ hoạt động của các hệ thống thông tin của ngành Bảo hiểm xã hội Việt Nam.

b) Các tổ chức, cá nhân có kết nối, chia sẻ, sử dụng, khai thác hệ thống thông tin của ngành Bảo hiểm xã hội Việt Nam.

c) Các tổ chức, cá nhân cung cấp dịch vụ đường truyền; dịch vụ an toàn thông tin mạng; cung cấp thiết bị, dịch vụ bảo hành và hỗ trợ kỹ thuật; dịch vụ quản lý, vận hành; dịch vụ nâng cấp, phát triển và bảo trì phục vụ hoạt động của các hệ thống thông tin của ngành Bảo hiểm xã hội Việt Nam (sau đây gọi chung là Đơn vị cung cấp dịch vụ).

3. Các từ viết tắt

a) BHXH là chữ viết tắt của cụm từ "bảo hiểm xã hội".

b) CNTT là chữ viết tắt của cụm từ "công nghệ thông tin"

c) ATTT là chữ viết tắt của cụm từ "an toàn thông tin"

d) HTTT là chữ viết tắt của cụm từ "hệ thống thông tin"

đ) ƯCSC là chữ viết tắt của cụm từ "ứng cứu sự cố"

4. Giải thích từ ngữ

a) Cơ quan điều phối quốc gia (sau đây gọi là Cơ quan điều phối) là Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT/CC) thuộc Cục An toàn thông tin - Bộ Thông tin và Truyền thông.

b) Thường trực Ban Chỉ đạo ứng cứu khẩn cấp sự cố ATTT mạng ngành BHXH Việt Nam (sau đây gọi là Thường trực Ban Chỉ đạo) là Phó Tổng Giám đốc BHXH Việt Nam phụ trách lĩnh vực CNTT.

c) Trung tâm CNTT là Cơ quan thường trực về ứng cứu khẩn cấp sự cố ATTT mạng ngành BHXH Việt Nam.

d) Đội ứng cứu sự cố ATTT mạng ngành BHXH Việt Nam (sau đây gọi là Đội ứng cứu sự cố) là công chức, viên chức và lao động hợp đồng làm công tác ATTT mạng theo Quyết định số 987/QĐ-BHXH ngày 11/7/2024.

đ) Đơn vị vận hành HTTT là Trung tâm CNTT, Văn phòng, các đơn vị sự nghiệp trực thuộc BHXH Việt Nam, BHXH các tỉnh, thành phố trực thuộc Trung ương (sau đây gọi là BHXH tỉnh) có quản lý trực tiếp HTTT và các đơn vị được thuê vận hành HTTT.

e) Trung tâm NOC là Trung tâm vận hành HTTT ngành BHXH Việt Nam.

g) Giám sát an toàn HTTT (sau đây gọi là giám sát ATTT) là hoạt động lựa chọn đối tượng, công cụ giám sát, thu thập, phân tích thông tin trạng thái của đối tượng giám sát, báo cáo, cảnh báo hành vi xâm phạm ATTT hoặc có khả năng gây ra sự cố ATTT đối với HTTT.

h) Bộ phận tác nghiệp ứng cứu sự cố bảo đảm ATTT mạng (sau đây gọi tắt là Bộ phận tác nghiệp ƯCSC) gồm các đơn vị: Đội ứng cứu sự cố, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

II. QUY TRÌNH THỰC HIỆN

1. Nguyên tắc chung

Nguyên tắc điều phối, ƯCSC bảo đảm tuân thủ theo đúng quy định tại Điều 4 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ƯCSC ATTT mạng trên toàn quốc, cụ thể như sau:

a) Tuân thủ các quy định pháp luật về điều phối, ƯCSC ATTT mạng.

b) Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả.

c) Phối hợp chặt chẽ, chính xác, đồng bộ và hiệu quả giữa các cơ quan tổ chức, doanh nghiệp trong nước và nước ngoài.

d) ƯCSC trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản HTTT.

đ) Tuân thủ các điều kiện, nguyên tắc ưu tiên về duy trì hoạt động của HTTT đã được cấp thẩm quyền phê duyệt trong kế hoạch ứng phó sự cố.

e) Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

g) Bảo đảm bí mật thông tin biết được khi tham gia, thực hiện các hoạt động ƯCSC theo yêu cầu của Cơ quan điều phối hoặc cơ quan tổ chức, cá nhân gặp sự cố.

2. Quy trình ứng cứu sự cố an toàn thông tin mạng

a) Quy trình ƯCSC ATTT mạng nghiêm trọng: Thực hiện theo các bước tại Mục 2 Phụ lục kèm theo.

b) Quy trình ƯCSC ATTT mạng thông thường: Thực hiện theo các bước tại Mục 3 Phụ lục kèm theo.

III. TỔ CHỨC THỰC HIỆN

1. Trung tâm Công nghệ thông tin

a) Tổ chức triển khai quy trình ƯCSC ATTT mạng trong ngành BHXH Việt Nam.

b) Chủ trì, hướng dẫn thực hiện các quy trình ƯCSC ATTT trong ngành BHXH Việt Nam.

c) Theo dõi, đôn đốc, kiểm tra và đánh giá tình hình triển khai, tuân thủ quy trình ƯCSC ATTT mạng trong ngành BHXH Việt Nam.

d) Chủ trì, giám sát ATTT và thực hiện các quy trình ƯCSC ATTT tại các Trung tâm dữ liệu Ngành.

đ) Đề xuất, báo cáo Tổng Giám đốc BHXH Việt Nam xem xét, điều chỉnh quy trình ƯCSC ATTT mạng trong ngành BHXH Việt Nam khi có thay đổi về chính sách và yêu cầu thực tế triển khai ứng dụng CNTT phát triển Chính phủ số và bảo đảm ATTT mạng tại BHXH Việt Nam.

2. Đơn vị vận hành hệ thống thông tin

a) Tuân thủ triển khai quy trình ƯCSC ATTT mạng trong ngành BHXH Việt Nam.

b) Phối hợp với Trung tâm CNTT trong quá trình ƯCSC ATTT trong ngành BHXH Việt Nam.

c) Chủ trì trong việc triển khai các biện pháp giám sát ATTT tại đơn vị và các đơn vị trực thuộc.

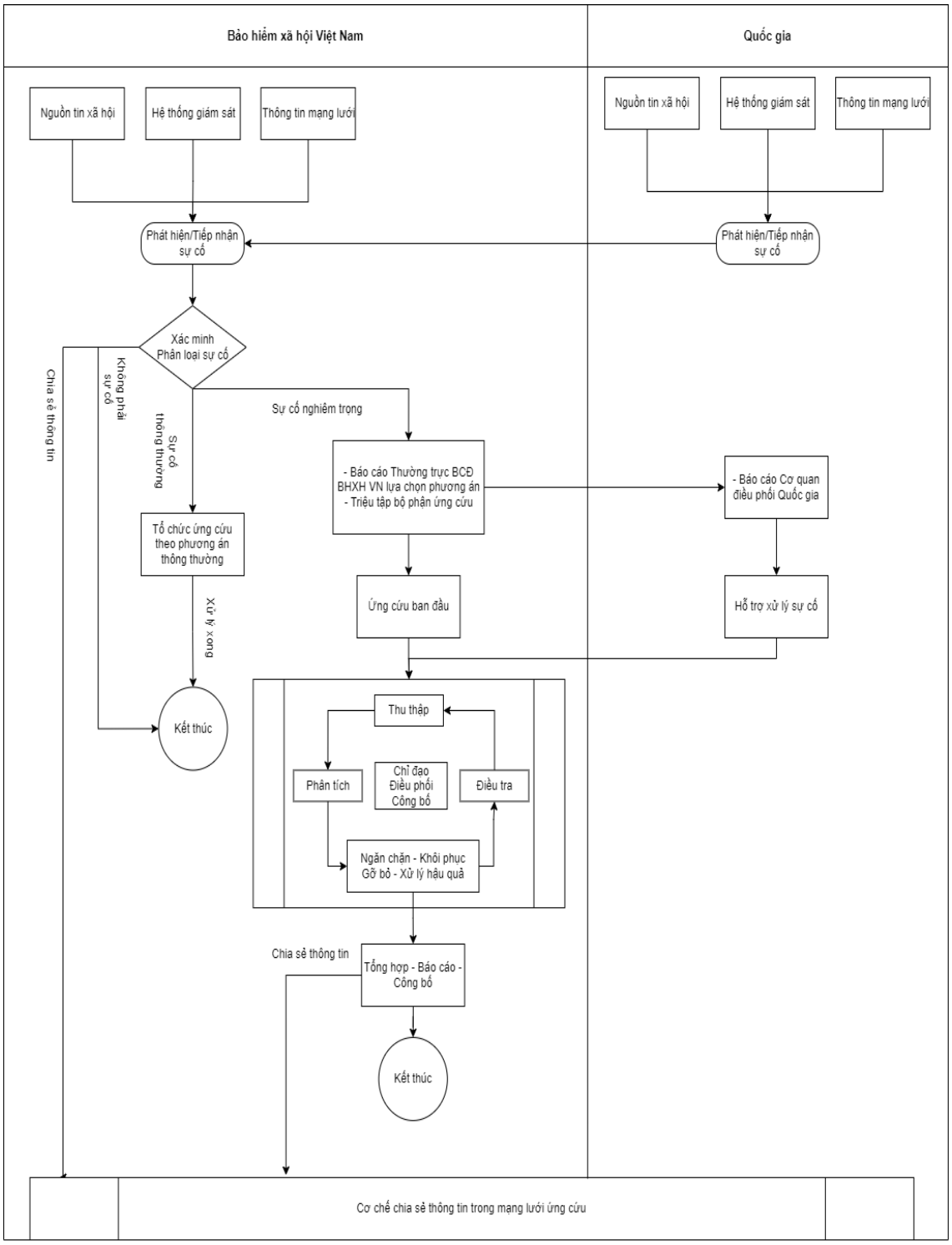
3. Đội ứng cứu sự cố

a) Chủ trì các hoạt động ƯCSC theo các quy trình ƯCSC ATTT trong ngành BHXH Việt Nam.

b) Phối hợp với Trung tâm CNTT trong quá trình ƯCSC ATTT trong ngành BHXH Việt Nam./.

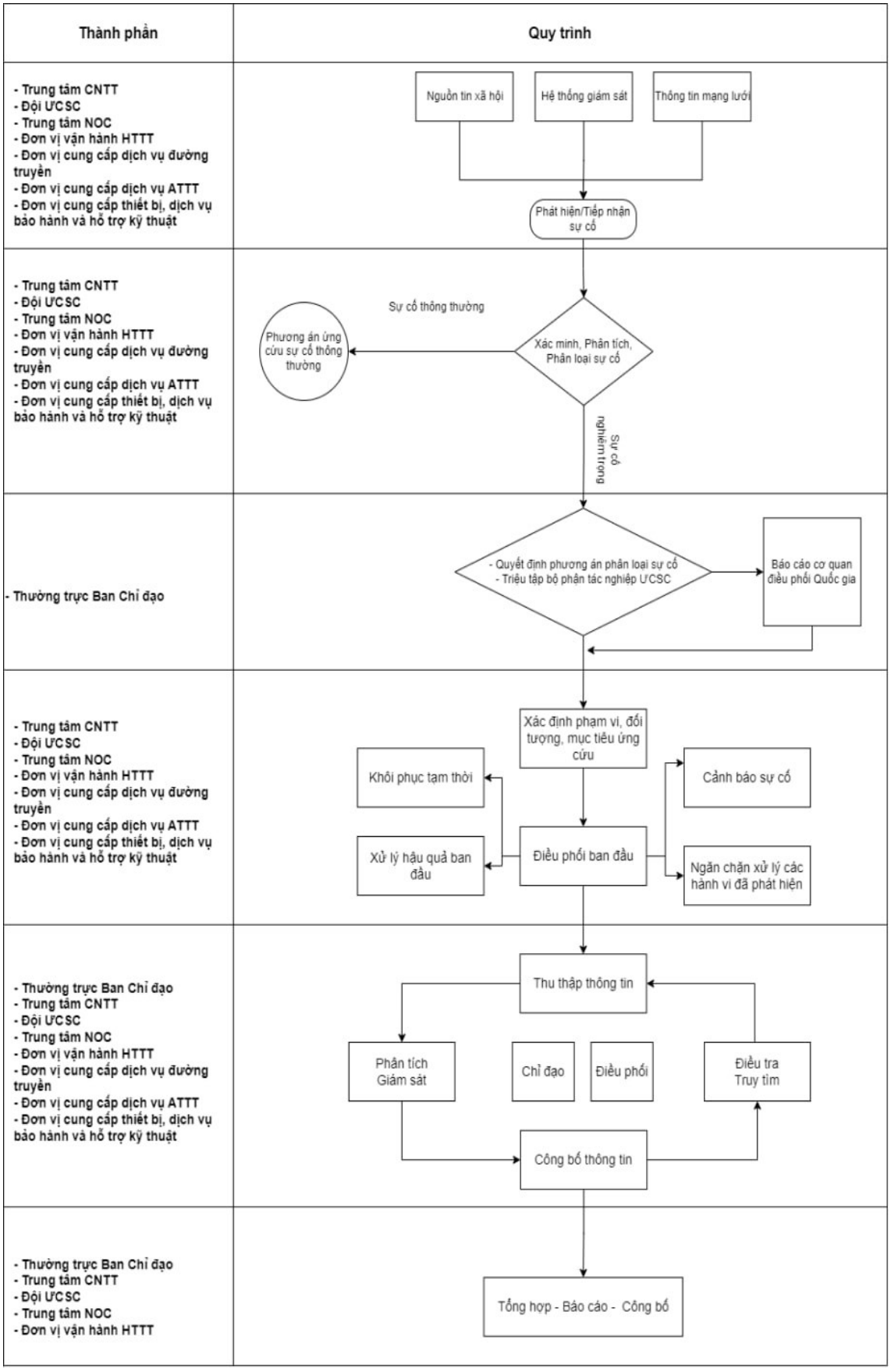
Phụ lục
QUY TRÌNH ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG NGÀNH BẢO HIỂM XÃ HỘI VIỆT NAM

1. Quy trình tổng thể



Hình 1. Quy trình ứng cứu sự cố an toàn thông tin mạng tổng thể

2. Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng



Hình 2. Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng

Trường hợp có nhiều sự cố đơn lẻ xảy ra cùng lúc, thực hiện đồng thời các quy trình tương ứng với từng sự cố.

Đơn vị chủ trì có trách nhiệm chủ động trong các bước thực hiện, đơn vị phối hợp bố trí nguồn lực để sẵn sàng tham gia với đơn vị chủ trì.

Quy trình ƯCSC ATTT mạng nghiêm trọng bao gồm các bước sau:

2.1. Phát hiện hoặc tiếp nhận sự cố

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT, Trung tâm CNTT**.

b) Đơn vị phối hợp: Đội ƯCSC, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Đơn vị vận hành HTTT tin chịu trách nhiệm liên tục theo dõi, phát hiện các tấn công, sự cố đối với hệ thống được giao quản lý, vận hành. Trung tâm CNTT là đơn vị đầu mối tổ chức các hoạt động theo dõi, giám sát, phát hiện các sự cố, tấn công mạng trong ngành BHXH Việt Nam và tiếp nhận thông báo về sự cố ATTT mạng từ Cơ quan điều phối, nguồn xã hội, thông tin mạng lưới...

2.2. Xác minh, phân tích, đánh giá và phân loại sự cố

a) Đơn vị chủ trì: **Trung tâm CNTT**.

b) Đơn vị phối hợp: Đội ƯCSC, Trung tâm NOC, Đơn vị vận hành HTTT, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện:

- Xác minh sự cố: Trung tâm CNTT phối hợp cùng Đội ƯCSC, Trung tâm NOC, Đơn vị vận hành HTTT, Đơn vị cung cấp dịch vụ xác minh sự cố bao gồm các thông tin sau:

+ Tình trạng sự cố;

+ Mức độ sự cố;

+ Phạm vi ảnh hưởng của sự cố;

+ Đối tượng, địa điểm xảy ra sự cố.

- Phân loại sự cố: Trung tâm CNTT có trách nhiệm phân loại sự cố và triển khai tiếp sau khi xác minh được sự cố:

+ Trường hợp sự cố được phân loại thông thường thì Trung tâm CNTT thông báo cho các bên liên quan để tiếp tục triển khai theo phương án ƯCSC ATTT thông thường;

+ Trường hợp sự cố được phân loại nghiêm trọng thì Trung tâm CNTT báo cáo Thường trực Ban chỉ đạo và Cơ quan điều phối về sự cố nghiêm trọng cùng với các đề xuất: Phương án ứng cứu; Các đơn vị tham gia lực lượng ứng cứu; Nguồn lực cần thiết để ƯCSC; Dự kiến triệu tập Bộ phận tác nghiệp ƯCSC.

2.3. Quyết định lựa chọn phương án và triệu tập các thành viên của Bộ phận tác nghiệp ứng cứu sự cố

a) Đơn vị chủ trì: **Thường trực Ban chỉ đạo.**

b) Nội dung thực hiện: Thường trực Ban chỉ đạo căn cứ theo báo cáo của Trung tâm CNTT xem xét quyết định quyết định phương án ứng cứu khẩn cấp và triệu tập Bộ phận tác nghiệp ƯCSC để ứng cứu, xử lý sự cố. Tùy theo tình hình thực tế, các đơn vị thuộc Bộ phận tác nghiệp ƯCSC được huy động phù hợp với phương án ứng cứu được lựa chọn, đặc thù của sự cố.

2.4. Triển khai phương án ứng cứu ban đầu

a) Đơn vị chủ trì: **Trung tâm CNTT**.

b) Đơn vị phối hợp: Đội ƯCSC, Trung tâm NOC, Đơn vị vận hành HTTT, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Trung tâm CNTT phối hợp với Đơn vị vận hành HTTT, các đơn vị thuộc Bộ phận tác nghiệp ƯCSC tiến hành các biện pháp ứng cứu ban đầu gồm:

- Xác định phạm vi, đối tượng, mục tiêu cần ứng cứu:

+ Các sự cố liên quan đã xảy ra;

+ Đối tượng đang bị ảnh hưởng;

+ Phạm vi bị ảnh hưởng;

+ Các mục tiêu ưu tiên trong khắc phục sự cố (khôi phục hoạt động, bảo đảm bí mật dữ liệu; bảo đảm tính toàn vẹn dữ liệu);

+ Diễn biến tình hình và phương thức thủ đoạn tấn công;

+ Dự đoán các diễn biến tiếp theo có thể xảy ra.

- Điều phối các hoạt động ứng cứu ban đầu: Trung tâm CNTT thực hiện điều phối và chia sẻ thông tin, tài liệu liên quan đến tình huống ứng cứu cho các thành viên tham gia theo chức năng, nhiệm vụ được giao.

- Báo cáo sự cố trên mạng lưới ứng cứu quốc gia: Trung tâm CNTT (thành viên mạng lưới ƯCSC quốc gia) thực hiện báo cáo với Cơ quan điều phối hoặc cảnh báo có khả năng xảy ra các sự cố tương tự đến Ban Điều hành mạng lưới.

- Tiến hành các biện pháp khôi phục tạm thời: Trung tâm CNTT phối hợp với Bộ phận tác nghiệp ƯCSC, Đơn vị cung cấp dịch vụ và các cơ quan chức năng tiến hành khôi phục một số hoạt động, dữ liệu hoặc kết nối cần thiết nhất để giảm thiểu thiệt hại đối với HTTT, ảnh hưởng uy tín của cơ quan BHXH Việt Nam hoặc gây ảnh hưởng xấu tới xã hội.

- Xử lý hậu quả ban đầu: Trung tâm CNTT tiến hành các biện pháp khắc phục khẩn cấp các hậu quả, thiệt hại do tấn công mạng gây ra làm ảnh hưởng đến

người dân, xã hội, cơ quan, tổ chức khác theo yêu cầu của Thường trực Ban Chỉ đạo:

+ Sẵn sàng hệ thống, thiết bị, đường truyền, kết nối dự phòng;

+ Chuẩn bị thực hiện chuyển đổi hoạt động sang hệ thống, thiết bị dự phòng.

- Ngăn chặn, xử lý các hành vi đã được phát hiện: Trung tâm CNTT phối hợp các cơ quan chức năng triển khai hỗ trợ phát hiện và xử lý các nguồn phát tán tấn công, ngăn chặn các tấn công từ bên ngoài vào HTTT bị sự cố. Thường trực Ban Chỉ đạo chỉ đạo cung cấp các thông tin, chứng cứ liên quan đến các hành vi vi phạm pháp luật có yếu tố cấu thành tội phạm (nếu có) để các cơ quan chức năng thuộc Bộ Công an tiến hành điều tra, xác minh và ngăn chặn tội phạm.

2.5. Triển khai phương án ứng cứu khẩn cấp

2.5.1. Chỉ đạo xử lý sự cố

a) Đơn vị chủ trì: **Thường trực Ban chỉ đạo**.

b) Nội dung thực hiện: Thường trực Ban Chỉ đạo lựa chọn phương án ứng cứu và chỉ đạo Trung tâm CNTT, Bộ phận tác nghiệp ƯCSC triển khai theo phương án lựa chọn. Trong quá trình ứng cứu, tùy thuộc vào diễn biến tình hình thực tế, Thường trực Ban chỉ đạo có thể quyết định bổ sung thành phần tham gia tác nghiệp ứng cứu khẩn cấp.

2.5.2. Điều phối công tác ứng cứu

a) Đơn vị chủ trì: **Trung tâm CNTT**.

b) Nội dung thực hiện: Trung tâm CNTT thực hiện công tác điều phối ứng cứu và giám sát cơ chế phối hợp, chia sẻ thông tin theo phương án ứng cứu được lựa chọn.

2.5.3. Phát ngôn và công bố thông tin

a) Đơn vị chủ trì: **Thường trực Ban chỉ đạo**.

b) Nội dung thực hiện: Thường trực Ban Chỉ đạo chỉ định người phát ngôn, cung cấp thông tin; quyết định địa điểm, nội dung, thời điểm phát ngôn, cung cấp thông tin cho các cơ quan thông tin đại chúng, các cá nhân và tổ chức có liên quan đến sự cố.

2.5.4. Thu thập thông tin

a) Đơn vị chủ trì: **Trung tâm CNTT**.

b) Đơn vị phối hợp: Đội ƯCSC, Trung tâm NOC, Đơn vị vận hành HTTT, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Trung tâm CNTT cùng với Đơn vị vận hành HTTT phối hợp tiến hành thu thập, tổng hợp và chia sẻ, cung cấp thông tin cho các đơn vị thuộc thành phần tác nghiệp ƯCSC.

2.5.5. Phân tích, giám sát tình hình liên quan sự cố

a) Đơn vị chủ trì: **Trung tâm CNTT**.

b) Đơn vị phối hợp: Đội ƯCSC, Trung tâm NOC, Đơn vị vận hành HTTT, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện:

- Trung tâm CNTT phối hợp với Đơn vị vận hành HTTT thực hiện giám sát liên tục diễn biến sự cố và thông báo, cập nhật đến các đơn vị trong Bộ phận tác nghiệp ƯCSC.

- Các đơn vị thuộc Bộ phận tác nghiệp ƯCSC dựa trên các thông tin thu thập được, sử dụng các nguồn lực, phương tiện và các quy trình nghiệp vụ của mình để tiến hành phân tích sự cố. Kết quả phân tích sự cố được báo cáo Thường trực Ban Chỉ đạo, Trung tâm CNTT và chia sẻ trong nhóm tác nghiệp ứng cứu khẩn cấp để phục vụ ứng cứu, khắc phục sự cố.

2.5.6. Khắc phục sự cố

a) Đơn vị chủ trì: **Trung tâm CNTT**.

b) Đơn vị phối hợp: Đội ƯCSC, Trung tâm NOC, Đơn vị vận hành HTTT, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện:

- Sao lưu hệ thống trước và sau khi xử lý sự cố;

- Tiêu diệt các mã độc, phần mềm độc hại;

- Khôi phục hệ thống, dữ liệu và kết nối;

- Cấu hình hệ thống an toàn;

- Kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố;

- Khắc phục các điểm yếu ATTT;

- Bổ sung các thiết bị, phần cứng, phần mềm bảo đảm ATTT cho hệ thống;

- Triển khai theo dõi, giám sát, ngăn chặn khả năng lặp lại sự cố hoặc xảy ra các sự cố tương tự.

2.5.7. Ngăn chặn, xử lý hậu quả

a) Đơn vị chủ trì: **Trung tâm CNTT**.

b) Nội dung thực hiện:

- Trung tâm CNTT có trách nhiệm xử lý các hậu quả do sự cố HTTT của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác.

- Các đơn vị thuộc Bộ phận tác nghiệp ƯCSC dựa trên các kết quả phân tích, tiến hành điều tra và nghiệp vụ của mình để thực hiện ngăn chặn các hành vi gây ra sự cố hỗ trợ xử lý hậu quả, chống tái diễn tấn công.

2.5.8. Xác minh nguyên nhân và truy tìm nguồn gốc

a) Đơn vị chủ trì: **Trung tâm CNTT**.

b) Nội dung thực hiện: Trung tâm CNTT phối hợp với các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp phân tích sự cố, tham khảo các kết quả phân tích sự cố của các đơn vị khác, sử dụng các nguồn tin và quy trình nghiệp vụ của mình, chủ động điều tra chi tiết nguyên nhân và truy tìm nguồn gốc, tổng hợp, báo cáo Thường trực Ban Chỉ đạo và Cơ quan điều phối các thông tin liên quan, cụ thể bao gồm:

- Đối tượng bị tấn công;

- Phương thức thủ đoạn tấn công (quy trình, kỹ thuật, mẫu mã độc, phần mềm độc hại);

- Thời gian xảy ra sự cố;

- Các thiệt hại đã xảy ra;

- Đối tượng tấn công;

- Dự đoán khả năng xảy ra các sự cố tương tự và thiệt hại.

2.6. Đánh giá kết quả triển khai phương án ứng cứu khẩn cấp an toàn thông tin mạng

a) Đơn vị chủ trì: **Thường trực Ban Chỉ đạo**.

b) Nội dung thực hiện: Thường trực Ban Chỉ đạo trên cơ sở tổng hợp báo cáo phân tích của Trung tâm CNTT, tổ chức họp phân tích, đánh giá nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và các biện pháp bổ sung cho các sự cố tương tự.

2.7. Kết thúc hoạt động ứng cứu sự cố

a) Đơn vị chủ trì: **Trung tâm CNTT**.

b) Đơn vị phối hợp: Đội ƯCSC, Trung tâm NOC, Đơn vị vận hành HTTT, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Trung tâm CNTT căn cứ kết quả đánh giá của Thường trực Ban Chỉ đạo sẽ thực hiện hoàn tất các nhiệm vụ sau, kết thúc hoạt động ứng cứu sự cố khẩn cấp:

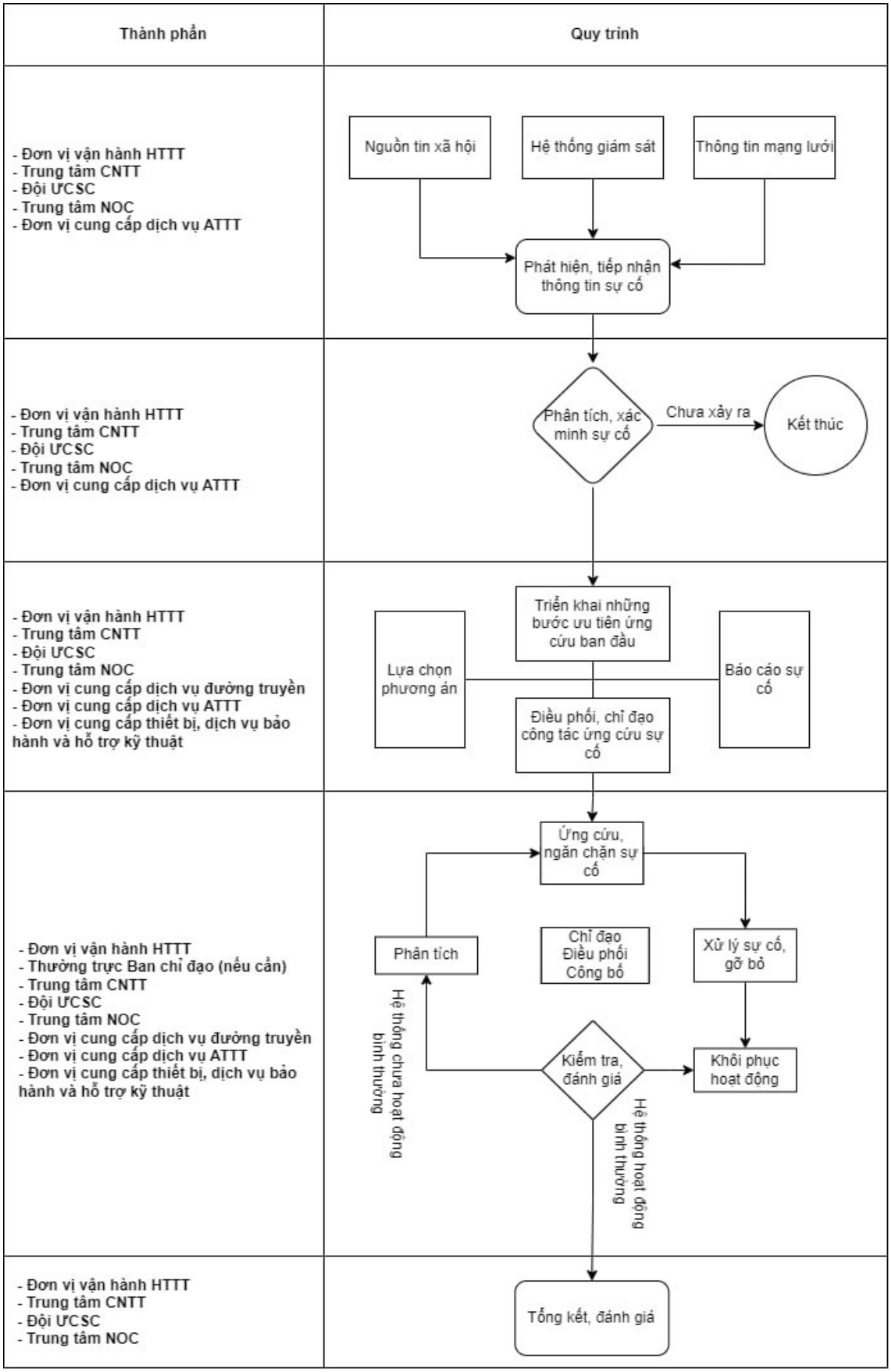
- Lưu hồ sơ, tài liệu lưu trữ;

- Xây dựng, đúc rút các bài học, kinh nghiệm;

- Đề xuất các kiến nghị về kỹ thuật, chính sách để hạn chế thiệt hại khi xảy ra các tấn công tương tự;

- Báo cáo cơ quan cấp trên, tổ chức họp báo hoặc gửi thông tin cho truyền thông nếu cần thiết.

3. Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường



Hình 3. Quy trình ứng cứu sự cố ATTT mạng thông thường

Trường hợp có nhiều sự cố đơn lẻ xảy ra cùng lúc, thực hiện đồng thời các quy trình tương ứng với từng sự cố.

Đơn vị chủ trì có trách nhiệm chủ động trong các bước thực hiện, đơn vị phối hợp bố trí nguồn lực để sẵn sàng tham gia với đơn vị chủ trì.

Quy trình ƯCSC ATTT mạng thông thường cụ thể gồm các bước sau:

3.1. Phát hiện, tiếp nhận sự cố

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT**.

b) Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC.

c) Nội dung thực hiện: Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố từ các nguồn bên trong và bên ngoài.

3.2. Triển khai các bước ưu tiên ứng cứu ban đầu

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT**.

b) Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố để phân tích, xác minh sự cố đã xảy ra.

3.3. Triển khai lựa chọn phương án ứng cứu

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT**.

b) Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Căn cứ theo kế hoạch ứng phó sự cố bảo đảm ATTT mạng trong ngành BHXH Việt Nam để lựa chọn phương án ngăn chặn và xử lý sự cố hoặc hướng dẫn của Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC; báo cáo, đề xuất Thường trực Ban Chỉ đạo xin ý kiến chỉ đạo (nếu cần).

3.4. Chỉ đạo xử lý sự cố (nếu cần)

a) Đơn vị chủ trì: **Thường trực Ban Chỉ đạo**.

b) Đơn vị phối hợp: Trung tâm CNTT.

c) Nội dung thực hiện: Thường trực Ban Chỉ đạo có ý kiến chỉ đạo Trung tâm CNTT, triệu tập thành viên Bộ phận tác nghiệp ƯCSC thuộc phạm vi quản lý triển khai công tác ứng cứu, xử lý sự cố; chỉ đạo, phân công hoạt động phát ngôn, cung cấp thông tin. Trong quá trình ứng cứu, tùy thuộc vào diễn biến tình hình thực tế, Thường trực Ban Chỉ đạo có thể quyết định bổ sung thành phần tham gia Bộ phận tác nghiệp ƯCSC, chỉ đạo điều chỉnh phương án ƯCSC.

3.5. Báo cáo sự cố

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT**.

b) Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Đơn vị vận hành HTTT báo cáo sự cố đến Trung tâm CNTT sau khi đã triển khai các bước ưu tiên ứng cứu ban đầu.

3.6. Điều phối công tác ứng cứu

a) Đơn vị chủ trì: **Thường trực Ban chỉ đạo, Trung tâm CNTT**.

b) Đơn vị phối hợp: Đơn vị vận hành HTTT, Đội ƯCSC, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Thường trực Ban chỉ đạo, Trung tâm CNTT thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ƯCSC.

3.7. Triển khai ứng cứu, ngăn chặn và xử lý sự cố

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT**.

b) Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện:

- Thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng;

- Triển khai phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến HTTT.

3.8. Xử lý sự cố

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT**.

b) Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Đơn vị vận hành HTTT phối hợp với Trung tâm CNTT, Đội ƯCSC, Đơn vị cung cấp dịch vụ triển khai tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại khắc phục các điểm yếu ATTT của HTTT sau khi đã triển khai ngăn chặn sự cố.

3.9. Khôi phục hoạt động hệ thống

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT**.

b) Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Đơn vị vận hành HTTT chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục HTTT dữ liệu và kết nối; cấu hình

hệ thống an toàn; bổ sung các thiết bị, phần cứng phần mềm bảo đảm ATTT cho HTTT.

3.10. Kiểm tra, đánh giá hệ thống thông tin

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT**.

b) Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC, Đơn vị cung cấp dịch vụ.

c) Nội dung thực hiện: Đơn vị vận hành HTTT và các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ HTTT sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và thực hiện các bước tương ứng để xử lý dứt điểm, khôi phục hoạt động bình thường của HTTT.

3.11. Tổng kết, đánh giá

a) Đơn vị chủ trì: **Đơn vị vận hành HTTT**.

b) Đơn vị phối hợp: Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC.

c) Nội dung thực hiện: Đơn vị vận hành HTTT phối hợp với Trung tâm CNTT, Đội ƯCSC, Trung tâm NOC triển khai tổng hợp toàn bộ các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ƯCSC; tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai báo cáo Thường trực Ban Chỉ đạo.