ỦY BAN NHÂN DÂN TỈNH BÌNH PHƯỚC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 877 /QĐ-UBND	*Bình Phước, ngày 26 tháng 05 năm 2023*

QUYẾT ĐỊNH
Ban hành Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Bình Phước

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015;

Căn cứ Luật Sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;

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

Căn cứ Luật An toàn thông tin ngày 19/11/2015;

Căn cứ Luật An ninh mạng ngày 12/6/2018;

Căn cứ Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng Chính phủ ban hành quy định về hệ thống phương án ứng cứu khẩn cấp đảm bảo an toàn thông tin mạng quốc gia;

Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 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 Quyết định số 12/2023/QĐ-UBND ngày 23/02/2023 của UBND tỉnh ban hành quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Sở Thông tin và Truyền thông;

Căn cứ Quyết định số 804/QĐ-UBND ngày 18/5/2023 của UBND tỉnh kiện toàn Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Bình Phước;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 31/TTr-STTTT ngày 06/4/2023.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Bình Phước.

Điều 2. Quyết định này có hiệu lực kể từ ngày ký và thay thế Quyết định số 395/QĐ-UBND ngày 07/3/2022 của UBND tỉnh ban hành Quy chế hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Bình Phước.

Điều 3. Chánh Văn phòng UBND tỉnh; Thủ trưởng các sở, ban, ngành tỉnh; Chủ tịch UBND các huyện, thị xã, thành phố; thành viên Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

Nơi nhận:
- Như Điều 3;
- Bộ TT&TT;
- TTTU, TT HĐND tỉnh, BTT UBMTTQVN tỉnh;
- CT, các PCT UBND tỉnh;
- LĐVP, các Phòng;
- Lưu: VT, KGVX, TD4.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Trần Tuyết Minh

ỦY BAN NHÂN DÂN TỈNH BÌNH PHƯỚC	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc

QUY CHẾ
Hoạt động của Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Bình Phước

(Ban hành kèm theo Quyết định số 877 /QĐ-UBND ngày 26/5/2023 của UBND tỉnh)

Chương I
QUY ĐỊNH CHUNG

Điều 1. Phạm vi và đối tượng áp dụng

1. Quy chế này quy định về nhiệm vụ, trách nhiệm, quyền hạn, nguyên tắc hoạt động và chế độ của Đội ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh Bình Phước.

2. Quy chế này được áp dụng cho Đội ứng cứu sự cố an toàn thông tin mạng và các cơ quan, tổ chức, cá nhân có liên quan trong hoạt động điều phối, ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh.

Điều 2. Giải thích từ ngữ

1. *Đội ứng cứu sự cố an toàn thông tin mạng (Đội ứng cứu sự cố)* là tổ chức/đơn vị do Chủ quản hệ thống thông tin thành lập nhằm triển khai các hoạt động, giải pháp sẵn sàng ứng phó hoặc ứng phó với các đe dọa, rủi ro; các lỗ hổng, điểm yếu; các sự cố đối với các hệ thống, cơ sở hạ tầng thông tin và không gian mạng trong phạm vi quản lý.

2. *Chủ quản Đội ứng cứu sự cố* là cơ quan ra quyết định thành lập Đội ứng cứu sự cố. Chủ quản Đội ứng cứu sự cố có thẩm quyền quyết định mô hình tổ chức, quyết định phân bổ nhân lực, vật lực và kinh phí hoạt động của Đội ứng cứu sự cố theo quy định pháp luật có liên quan.

3. *Vị trí chuyên trách về an toàn thông tin*: Đảm nhiệm nhóm công việc đặc trưng khác biệt, có cùng độ phức tạp, thuộc lĩnh vực an toàn thông tin; thường sử dụng cùng nhóm kiến thức và kỹ năng. Khác với vị trí việc làm chuyên môn, cơ quan nào cũng có như: quản lý nhân sự, tài chính,…

4. *Sự cố an toàn thông tin mạng* là sự kiện đã, đang xảy ra gây mất an toàn thông tin trên môi trường mạng (LAN, WAN, 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 mạng trong nước và trên thế giới.

5. *Ứng cứu sự cố an toàn thông tin mạng* là hoạt động nhằm xử lý, khắc phục sự cố gây mất an toàn thông tin mạng, gồm: theo dõi, thu thập, phân tích,

phát hiện, cảnh báo, kiểm tra, xác minh sự cố, ngăn chặn sự cố, khôi phục dữ liệu và khôi phục hoạt động bình thường của hệ thống thông tin.

Điều 3. Tổ chức Đội ứng cứu sự cố

Đội ứng cứu sự cố có chức năng giám sát, kiểm tra, thực hiện các hoạt động ứng cứu sự cố ATTT các cơ quan Đảng, Đoàn thể, Nhà nước trên địa bàn tỉnh; cảnh báo kịp thời các vấn đề an toàn, an ninh thông tin; triển khai thực hiện các tiêu chuẩn kỹ thuật quốc gia về an toàn an ninh thông tin; phối hợp, xây dựng các tiêu chuẩn kỹ thuật ATTT thích hợp trên địa bàn tỉnh; là đầu mối thực hiện hợp tác với các tổ chức ATTT Quốc gia, Cục An toàn thông tin, Hiệp hội An toàn thông tin Việt Nam khu vực phía Nam, Cụm thành viên mạng lưới ứng cứu sự cố số 9.

Điều 4. Nhiệm vụ và quyền hạn của Đội ứng cứu sự cố

1. Hỗ trợ các sở, ban, ngành tỉnh; UBND các huyện, thị xã, thành phố và đơn vị liên quan trong công tác đảm bảo an toàn thông tin mạng (ATTTM) trong hoạt động ứng dụng công nghệ thông tin (CNTT) và tổ chức ứng cứu các sự cố ATTTM trên địa bàn tỉnh.

2. Là đầu mối của tỉnh, có nhiệm vụ liên kết, phối hợp với các đơn vị trong mạng lưới ứng cứu sự cố quốc gia (dưới sự điều phối của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT) trong việc thu thập thông tin, kịp thời cảnh báo sự cố và các điểm yếu, lỗ hổng bảo mật, các nguồn tấn công mạng để các cơ quan, đơn vị chủ động phòng chống, giảm thiểu rủi ro, mất ATTTM.

3. Tham gia các khóa huấn luyện, diễn tập năng lực và phát triển nhân lực, Đội ứng cứu sự cố.

4. Tham gia hoạt động ứng cứu khẩn cấp sự cố ATTTM quốc gia khi có yêu cầu từ Bộ Thông tin và Truyền thông hoặc Cơ quan điều phối quốc gia về ứng cứu sự cố (Cục An toàn thông tin, Bộ Thông tin và Truyền thông).

5. Tham gia các hoạt động của Mạng lưới ứng cứu sự cố ATTTM quốc gia; tham gia hoạt động phòng, chống chiến tranh thông tin, chiến tranh không gian mạng khi có yêu cầu của cơ quan chức năng.

6. Được sự đồng ý (bằng văn bản có ký tên, đóng dấu) của lãnh đạo đơn vị bị sự cố, các thành viên Đội ứng cứu sự cố có quyền truy cập vào hệ thống mạng, hệ thống ứng dụng CNTT, cơ sở dữ liệu, log file để phân tích, truy vết và thực hiện dưới sự giám sát của đơn vị bị sự cố.

7. Báo cáo định kỳ 06 tháng (trước ngày 20/6), 01 năm (trước ngày 15/12) theo quy định gửi cơ quan điều phối quốc gia, UBND tỉnh hoặc báo cáo đột xuất khi có yêu cầu.

Chương II

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

Điều 5. Nguyên tắc hoạt động

1. Điều phối hoạt động ứng cứu sự cố theo phân cấp, trong phạm vi của tỉnh.

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

3. Thông tin được trao đổi, cung cấp trong quá trình điều phối, xử lý sự cố phải được bảo đảm bí mật theo yêu cầu của cơ quan, đơn vị gặp sự cố, trừ khi sự cố xảy ra có liên quan tới nhiều đối tượng khác cần phải cảnh báo hoặc phối hợp.

4. Việc trao đổi thông tin trong hoạt động điều phối phải được thực hiện bằng một hoặc nhiều hình thức như: Công văn, thư điện tử, điện thoại, fax... Thành viên Đội ứng cứu sự cố khi tiếp nhận thông tin phải chủ động xác thực đối tượng gửi nhằm bảo đảm tính chính xác của thông tin tiếp nhận.

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

Điều 6. Chế độ làm việc

1. Khi xảy ra sự cố phải ưu tiên cho hoạt động của Đội ứng cứu sự cố, thực hiện nghiêm sự triệu tập, điều phối của Đội trưởng hoặc Đội phó khi được ủy quyền.

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

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

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

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

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

b) Đội phó Thường trực ký ban hành văn bản thực hiện văn bản điều phối sự cố từ cơ quan cấp trên (Bộ Thông tin và Truyền thông, Cục An toàn thông tin, Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam - VNCERT).

Điều 7. Kinh phí hoạt động

Hằng năm, căn cứ nguồn thu ngân sách tỉnh, Sở Tài chính tham mưu cấp có thẩm quyền phê duyệt kinh phí hoạt động của Đội ứng cứu sự cố và được bố trí vào dự toán của Sở Thông tin và Truyền thông.

Chương III
HOẠT ĐỘNG ĐIỀU PHỐI, ỨNG CỨU SỰ CỐ

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

1. Các hình thức thông báo, báo cáo sự cố

a) Hình thức thông báo sự cố: Bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện.

b) Hình thức báo cáo sự cố: Bằng văn bản giấy hoặc văn bản điện tử (có ký tên, đóng dấu hoặc chữ ký số của người có thẩm quyền).

2. Cơ quan, địa phương khi gặp sự cố không tự khắc phục được cần thông báo hoặc báo cáo sự cố tới thường trực Đội ứng cứu sự cố hoặc thành viên Đội ứng cứu sự cố *(theo mẫu Phụ lục I, II)*.

3. Khi phát hiện và nhận thấy sự cố nghiêm trọng, cơ quan, đơn vị phải có trách nhiệm thông báo ngay cho Thường trực Đội ứng cứu sự cố.

4. Nội dung thông báo sự cố gồm: Tên, địa chỉ đơn vị, cá nhân thông báo sự cố; tên hoặc tên miền, địa chỉ IP của hệ thống thông tin bị sự cố; tên địa chỉ của đơn vị, cá nhân vận hành và cơ quan chủ quản hệ thống thông tin bị sự cố (nếu biết); mô tả sự cố và thời điểm phát hiện sự cố; kết quả xử lý sự cố đề xuất, kiến nghị và các thông tin liên quan khác (nếu có).

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

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

Điều 9. Quy trình ứng cứu sự cố an toàn thông tin mạng

1. Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố.

a) Tiếp nhận, xác minh sự cố.

b) Triển khai các bước ưu tiên ứng cứu ban đầu.

c) Triển khai lựa chọn phương án ứng cứu.

d) Chỉ đạo xử lý sự cố (nếu cần).

đ) Báo cáo sự cố.

e) Điều phối công tác ứng cứu.

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

a) Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng.

b) Triển khai phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin.

3. Xử lý sự cố, gỡ bỏ và khôi phục.

a) Xử lý sự cố, gỡ bỏ.

b) Khôi phục.

c) Kiểm tra, đánh giá hệ thống thông tin.

4. Tổng kết, đánh giá.

Điều 10. Ứng cứu sự cố

1. Đưa ra cảnh báo: làm đầu mối tiếp nhận cảnh báo của các cơ quan an ninh thông tin cấp trên. Xây dựng chương trình cảnh báo các lỗ hổng bảo mật đến các cơ quan, đơn vị.

2. Xử lý các lỗi và lỗ hổng bảo mật: nghiên cứu, báo cáo các lỗ hổng cho các đơn vị ATTT cấp tỉnh; trực tiếp tiếp nhận xử lý bảo mật từ đơn vị cấp trên. Trực tiếp, hướng dẫn các đơn vị xử lý các lỗ hổng bảo mật xảy ra trong hệ thống thông tin.

3. Kiểm tra, đánh giá, tư vấn bảo mật: kiểm tra, đánh giá công tác đảm bảo an toàn, an ninh tại đơn vị, hỗ trợ các đơn vị xây dựng các chương trình bảo mật.

4. Xây dựng, phát triển công cụ bảo mật.

5. Phân tích rủi ro: dựa trên công tác kiểm tra đánh giá an toàn tại các đơn vị đưa ra các cảnh báo về nguy cơ mất ATTT.

6. Điều tra sự cố: kịp thời xử lý, phối hợp với các cơ quan chức năng điều tra các sự cố, cuộc tấn công vào hệ thống thông tin của các cơ quan, đơn vị.

Điều 11. Điều phối ứng cứu sự cố

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

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

2. Thành viên Đội ứng cứu sự cố tiếp nhận thông báo điều phối; phối hợp chặt chẽ với đơn vị xảy ra sự cố và các thành viên cùng tham gia ứng cứu tổ chức thực hiện hoạt động ứng cứu theo quy trình điều phối quy định tại Điều 11, Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền

thông; báo cáo kết quả thực hiện cho Đội trưởng *(qua Thường trực Đội ứng cứu sự cố)*.

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

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

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

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

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

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

Điều 12. Đào tạo, hướng dẫn

- Xây dựng kế hoạch đào tạo ngắn hạn, dài hạn cho cán bộ chuyên trách CNTT tại các đơn vị bao gồm các cơ quan chuyên trách CNTT.

- Đào tạo, hướng dẫn công tác đảm bảo an toàn an ninh thông tin cho các cán bộ chuyên trách CNTT.

Chương IV

TRÁCH NHIỆM CỦA TỔ CHỨC, CÁ NHÂN

Điều 13. Văn phòng Thường trực Đội ứng cứu sự cố *(đặt tại Sở Thông tin và Truyền thông)*

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

- Số điện thoại thường trực: 02713.888.207.

- Email: stttt@binhphuoc.gov.vn.

Điều 14. Trách nhiệm và quyền hạn của Sở Thông tin và Truyền thông

1. Được quyền điều động các thành viên Đội ứng cứu sự cố nhằm thực hiện hoặc phối hợp thực hiện việc ngăn chặn, xử lý, khắc phục sự cố ATTTM.

2. Đầu mối liên lạc ứng cứu sự cố trên địa bàn tỉnh và trong mạng lưới ứng cứu sự cố ATTTM trên toàn quốc.

3. Theo dõi, cập nhật, thông báo kịp thời thông tin liên hệ của thành viên Đội ứng cứu sự cố của các cơ quan, đơn vị trên địa bàn tỉnh. Đề xuất, trình cấp có thẩm quyền kiện toàn khi có sự thay đổi nhân sự.

4. Thực hiện báo cáo định kỳ và đột xuất khi có yêu cầu về hoạt động tiếp nhận và xử lý sự cố cho UBND tỉnh, Cơ quan điều phối cấp trên, Bộ Thông tin và Truyền thông và cơ quan cấp trên khác có thẩm quyền.

Điều 15. Trách nhiệm và quyền hạn của Đội trưởng

1. Chịu trách nhiệm toàn bộ về hoạt động của Đội ứng cứu sự cố; chủ trì các cuộc họp, điều phối, quyết định tổ chức ứng cứu; triệu tập các thành viên để xử lý và khắc phục sự cố ATTTM.

2. Chủ trì tổ chức ứng cứu sự cố ATTTM trên địa bàn tỉnh, điều phối, phân công các thành viên trong Đội ứng cứu sự cố tham gia ứng cứu khi có sự cố xảy ra. Là đầu mối liên hệ, phối hợp với Trung tâm ứng cứu khẩn cấp máy tính Việt Nam - VNCERT, các doanh nghiệp cung cấp dịch vụ Internet và các đơn vị liên quan.

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

Điều 16. Trách nhiệm và quyền hạn của Đội phó

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

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

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

Điều 17. Trách nhiệm và quyền hạn của các thành viên Đội ứng cứu sự cố

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

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

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

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

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

6. Tiếp nhận đầy đủ, chính xác thông tin về sự cố được quy định tại khoản 4, Điều 8 Quy chế này và thông báo kịp thời cho Đội trưởng để thực hiện công tác điều phối ứng cứu sự cố.

7. Tham gia góp ý, đề xuất xây dựng Kế hoạch hoạt động hằng năm của Đội ứng cứu sự cố; tham gia các hoạt động diễn tập ứng cứu sự cố, các khóa đào tạo, bồi dưỡng về an toàn thông tin và ứng cứu sự cố do Sở Thông tin và Truyền thông triệu tập. Tham mưu lãnh đạo thực hiện tốt công tác đảm bảo an toàn thông tin tại cơ quan, đơn vị.

8. Kịp thời thông báo sự cố xảy ra gửi về Đội ứng cứu sự cố để phối hợp xử lý; định kỳ (06 tháng, 01 năm) báo cáo tổng hợp về hoạt động tiếp nhận và xử lý sự cố *(theo mẫu Phụ lục III)*.

Điều 18. Trách nhiệm của cơ quan quản lý thành viên của Đội ứng cứu sự cố

- Thủ trưởng các cơ quan, đơn vị có trách nhiệm tạo điều kiện và ưu tiên cho thành viên đội ứng cứu sự cố thuộc đơn vị mình quản lý thực hiện các hoạt động của Đội ứng cứu sự cố khi được triệu tập, điều phối.

- Kịp thời thông báo về Sở Thông tin và Truyền thông cập nhật danh sách thành viên tham gia Đội ứng cứu sự cố khi có thay đổi.

Chương V
TỔ CHỨC THỰC HIỆN

Điều 19. Tổ chức thực hiện

1. Sở Thông tin và Truyền thông chủ trì tổ chức, kiểm tra, hướng dẫn Đội ứng cứu và các cơ quan, đơn vị có liên quan thực hiện Quy chế này; kịp thời phát hiện và phối hợp với cơ quan chức năng tham mưu xử lý những trường hợp vi phạm.

2. Căn cứ kết quả hoạt động của mỗi thành viên, Đội ứng cứu sự cố xem xét, đề nghị cấp có thẩm quyền khen thưởng, kỷ luật theo quy định.

3. Trong quá trình triển khai thực hiện Quy chế, nếu có vấn đề phát sinh, vướng mắc, các cơ quan, đơn vị, tổ chức, cá nhân phản ánh với UBND tỉnh (qua Sở Thông tin và Truyền thông) để xem xét, sửa đổi, bổ sung./.

Phụ lục I

MẪU BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG

(Ban hành kèm theo Quyết định số...../QĐ-UBND ngày .../5/2023 của UBND tỉnh)

BÁO CÁO BAN ĐẦU SỰ CỐ MẠNG
THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO SỰ CỐ

Tên tổ chức/cá nhân báo cáo sự cố (*).....……
Địa chỉ: (*) .....……
Điện thoại (*) .....……
Email (*).....……
NGƯỜI LIÊN HỆ
Họ và tên (*).....Chức vụ: .....……
Điện thoại (*)……...Email (*)…….....……
THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*
Tên hệ thống bị sự cố	*Điền tên hệ thống bị sự cố và tên miền, địa chỉ ip liên quan*
Phân loại cấp độ của hệ thống thông tin (nếu có)	□ Cấp độ 1 □ Cấp độ 2 □ Cấp độ 3 □ Cấp độ 4 □ Cấp độ 5
Tổ chức cung cấp dịch vụ an toàn thông tin (nếu có):	*Điền tên nhà cung cấp ở đây*
Tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)	*Điền tên nhà cung cấp ở đây*
Điền tên nhà cung cấp ở đây	*Điền thông tin ở đây*

Mô tả sơ bộ sự cố (*)

Đề nghị cung cấp một bản tóm tắt ngắn gọn về sự cố, bao gồm đánh giá sơ bộ cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Cũng vui lòng xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố:

……
……
……
……

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

HIỆN TRẠNG SỰCỐ (*)

□ Đã được xử lý . □ Chưa được xử lý

CÁCH THỨC PHÁT HIỆN * *(Đánh đấu 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... ⋮..... .. ..

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 BỔ SUNG 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 hiển 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

KIẾN NGHỊ, ĐỀ XUẤT HỖ TRỢ

Mô tả về đề xuất, kiến nghị *Đề nghị cung cấp tóm lược về các kiến nghị và đề xuất hỗ trợ ứng cứu (nếu có)* …… …… …… …… ……

…… ……

THỜI GIAN THỰC HIỆN BÁO CÁO SỰ CỐ*:
(ngày/tháng/năm/giờ/phút)

CÁ NHÂN/NGƯỜI ĐẠI DIỆN
THEO PHÁPLUẬT
(Ký tên, đóng dấu)

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 VNCERT (www.vncert.gov vn)*

Phụ lục II

MẪU BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

(Ban hành kèm theo Quyết định số /QĐ-UBND ngày…/5/2023 của UBND tỉnh)

BÁO CÁO KẾT THÚC ỨNG PHÓ SỰ CỐ

THÔNG TIN VỀ TỔ CHỨC/CÁ NHÂN BÁO CÁO

- Tên tổ chức/cá nhân báo cáo sự cố (*)
- Địa chỉ: (*) ..... ……
- Điện thoại (*)……...
- Email (*)…… ..... ……

KÝ HIỆU BÁO CÁO BAN ĐẦU SỰ CỐ: Số ký hiệu Ngày báo cáo: / /202..

THÔNG TIN CHI TIẾT VỀ HỆ THỐNG BỊ SỰ CỐ

Tên đơn vị vận hành hệ thống thông tin (*):	*Điền tên đơn vị vận hành hoặc được thuê vận hành hệ thống thông tin*
Cơ quan chủ quản:	*Điền tên cơ quan chủ quản*
Tên hệ thống bị sự cố	*Điền tên hệ thắng bị sự cố*
Phân loại cấp độ của hệ thống thông tin, (nếu có)	□ Cấp độ 1 □ Cấp độ 2 □ Cấp độ 3 □ Cấp độ 4 □ Cấp độ 5

Tên/Mô tả về sự cố …… …… …… …… ……..

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

Kết quả xự lý sự cố
Cung cấp, tóm tắt tổng quát về những gì đã xảy ra và cách thức giải quyết, đề xuất giải pháp ứng cứu ứng sự cố nhằm xử lý nhanh sự cố, giảm nhẹ rủi ro và thiệt hại đối với sự cố tương tự trong tương lai …… …… ……

……

Các tài liệu đính kèm
Liệt kê các tài liệu liên quan (báo cáo diễn biến sự cố; phương án xử lý, log file...)

CÁ NHÂN/NGƯỜI ĐẠI DIỆN THEO PHÁPLUẬT
(Ký tên, đóng dấu)

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

Phụ lục III

MẪU BÁO CÁO ĐỊNH KỲ

(Ban hành kèm theo Quyết định số /QĐ-UBND ngày…/5/2023 của UBND tỉnh)

Kính gửi: Sở Thông tin và Truyền thông.

BÁO CÁO TỔNG HỢP (06 THÁNG, 01 NĂM VỀ HOẠT ĐỘNG TIẾP NHẬN VÀ XỬ LÝ SỰ CỐ

□ Từ tháng ……/20 ... đến tháng ..../20...

Tên cơ quan/tổ chức:..... .. ..

Địa chỉ:.....…..... ...……

1. Số lượng sự cố và cách thức xử lý

Loại sự cố/tấn công mạng	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 lý	Thiệt hại ước tính
Từ chối dịch vụ						
Tấn công giả mạo						
Tấn cộng sử dụng mã độc						
Truy cập trái phép, chiếm quyền điều khiển						
Thay đổi giao diện						
Mã hóa phần mềm, dữ liệu, thiết bị						
Phá hoại thông tin, dữ liệu, phần mềm						
Nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu						
Tấn công tổng hợp sử dụng kết hợp nhiều hình thức						
Các hình thức tấn công 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 .....

NGƯỜI ĐẠI DIỆN THEO PHÁP LUẬT

(Ký tên, đóng dấu)