ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 5479/KH-UBND	*Khánh Hòa, ngày 08 tháng 5 năm 2025*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2025

Thực hiện 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 bảo đảm an toàn thông tin mạng quốc gia; Quyết định số 1017/QĐ-TTg ngày 14/8/2018 của Thủ tướng Chính phủ phê duyệt Đề án giám sát an toàn thông tin mạng đối với hệ thống, dịch vụ công nghệ thông tin phục vụ Chính phủ điện tử đến năm 2020, định hướng đến năm 2025; triển khai Kế hoạch số 13784/KH-UBND ngày 31/12/2020 của UBND tỉnh về ứng dụng công nghệ thông tin, phát triển chính quyền số và bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan nhà nước tỉnh Khánh Hòa giai đoạn 2021-2025; xét Tờ trình số 3784/TTr-CAT(ANM) ngày 24/4/2025 của Công an tỉnh, UBND tỉnh Khánh Hòa ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2025, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn thông tin cho các hệ thống thông tin quan trọng trên địa bàn tỉnh; bảo đảm khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trong hệ thống mạng; triển khai thực hiện có hiệu quả các giải pháp ứng phó, khắc phục khi xảy ra sự cố mất an toàn thông tin mạng.

- Nâng cao năng lực giám sát an toàn thông tin mạng trên địa bàn tỉnh để tăng cường khả năng phát hiện sớm, cảnh báo kịp thời, chính xác về các sự kiện, rủi ro, dấu hiệu, hành vi, mức độ xâm hại, nguy cơ, điểm yếu, lỗ hổng gây mất an toàn thông tin mạng đối với các hệ thống thông tin quan trọng, ứng dụng dịch vụ công nghệ thông tin phục vụ chính phủ điện tử của tỉnh.

- Tạo chuyển biến mạnh mẽ trong nhận thức về việc chủ động phối hợp bảo vệ an toàn thông tin đối với lực lượng công chức, viên chức, người lao động; nâng cao ý thức, năng lực của người dùng cuối trong việc truy cập, khai thác vào các hệ thống thông tin trọng yếu của tỉnh, góp phần quan trọng trong việc bảo đảm an toàn thông tin mạng trên địa bàn tỉnh.

- Bảo đảm các nguồn lực và các điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả các phương án ứng cứu khẩn cấp sự cố an toàn thông tin mạng, giảm thiểu thiệt hại xuống mức thấp nhất có thể.

2. Yêu cầu

- Căn cứ trên kết quả khảo sát, đánh giá các nguy cơ, sự cố mất an toàn thông tin mạng của hệ thống thông tin các cơ quan nhà nước trên địa bàn tỉnh để đưa ra phương án ứng phó phù hợp và thực hiện ứng cứu khẩn cấp sự cố kịp thời, hiệu quả.

- Phương án ứng phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra các tiêu chí để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra.

- Xác định cụ thể các nguồn lực, giải pháp tổ chức thực hiện và kinh phí để triển khai các nội dung của Kế hoạch, bảo đảm khả thi, hiệu quả.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác bảo đảm an toàn thông tin giữa các cơ quan nhà nước trên địa bàn tỉnh; tận dụng sự phối hợp, hỗ trợ của các đơn vị nghiệp vụ của Bộ Công an.

II. NHIỆM VỤ TRIỂN KHAI

1. Triển khai các nhiệm vụ khi chưa có sự cố xảy ra

a) Tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng

- Nội dung thực hiện: Tổ chức tuyên truyền, phổ biến, hướng dẫn nội dung của Luật An toàn thông tin mạng và các quy định về công tác ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng.

- Đơn vị thực hiện: Công an tỉnh.

- Đơn vị phối hợp: Các sở, ban, ngành, UBND địa phương và các đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

b) Triển khai các chương trình đào tạo, bồi dưỡng kỹ năng đánh giá, ứng cứu khẩn cấp sự cố

- Nội dung thực hiện: Tổ chức huấn luyện, diễn tập các phương án ứng phó và thực hiện ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; đào tạo nâng cao kỹ năng, biện pháp nghiệp vụ phối hợp ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố; tham gia huấn luyện, đào tạo, bồi dưỡng, diễn tập vùng, miền, quốc gia, quốc tế theo triệu tập của cơ quan cấp trên.

- Đơn vị thực hiện: Công an tỉnh; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (*sau đây viết tắt là Đội UCKCSC*).

- Đơn vị phối hợp: Đơn vị chủ quản, quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương); Các đơn vị nghiệp vụ của Bộ Công an.

- Thời gian thực hiện: Trong năm 2025.

c) Triển khai phòng ngừa sự cố, giám sát phát hiện sớm sự cố

- Nội dung thực hiện:

+ Tiếp tục triển khai mở rộng hệ thống Trung tâm Giám sát an toàn thông tin mạng (SOC), kết nối Trung tâm Giám sát an toàn không gian mạng quốc gia, mở rộng phạm vi giám sát đến các cơ quan chuyên môn cấp tỉnh và các địa phương; tổ chức giám sát, phát hiện sớm các nguy cơ, sự cố; kiểm tra, đánh giá an toàn thông tin mạng và rà quét, bóc gỡ, phân tích, xử lý mã độc; phòng ngừa sự cố, quản lý rủi ro; nghiên cứu, phân tích, xác minh, cảnh báo sự cố, rủi ro an toàn thông tin mạng, phần mềm độc hại; xây dựng, áp dụng quy trình, quy định, tiêu chuẩn an toàn thông tin; tuyên truyền, nâng cao nhận thức về nguy cơ, sự cố, tấn công mạng.

+ Rà soát đánh giá tình hình, công tác phòng ngừa sự cố trong thời gian qua, xác định những lĩnh vực trọng tâm, trọng điểm, có nguy cơ cao, từ đó tập trung triển khai các biện pháp bảo vệ, phòng ngừa; chú ý sắp xếp, bố trí cán bộ đủ năng lực chuyên môn, có phẩm chất tốt để đảm nhiệm những vị trí quan trọng trong quản lý, vận hành các hệ thống thông tin. Chú trọng vấn đề nâng cấp giao thức bảo mật cho các trang/cổng thông tin điện tử, cơ sở hạ tầng mạng trong hệ thống thông tin của các cơ quan nhà nước thuộc tỉnh.

- Đơn vị thực hiện: Công an tỉnh, Đội UCKCSC; Đơn vị chủ quản, quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

- Đơn vị phối hợp: Các đơn vị nghiệp vụ của Bộ Công an.

- Thời gian thực hiện: Thường xuyên trong năm.

d) Triển khai các điều kiện sẵn sàng ứng phó, ứng cứu, khắc phục sự cố

- Nội dung thực hiện: Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, gia hạn bản quyền phần mềm phục vụ công tác ứng cứu khẩn cấp, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng các nguồn lực và tài chính để sẵn sàng ứng phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của Đội UCKCSC; thuê dịch vụ kỹ thuật và tổ chức, duy trì đội chuyên gia ứng cứu sự cố; tổ chức và tham gia các hoạt động của mạng lưới ứng cứu sự cố. Nghiên cứu xây dựng phương án về nhân lực, trang thiết bị, phần mềm, phương tiện, công cụ và dự kiến kinh phí để thực hiện, ứng phó, ứng cứu, xử lý theo hướng linh hoạt, hiệu quả đối với từng tình huống sự cố cụ thể.

- Đơn vị thực hiện: Công an tỉnh; Đội UCKCSC; Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành,địa phương).

- Đơn vị phối hợp: Các đơn vị nghiệp vụ của Bộ Công an và các đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

e) Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

- Nội dung thực hiện: Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng đối với hệ thống thông tin; đánh giá, dự báo các nguy cơ, sự cố hệ thống thông tin có thể xảy ra; dự báo đối tượng có thể tấn công, phá hoại gây ra sự cố mất an toàn thông tin mạng; đánh giá, dự báo các hậu quả, thiệt hại, tác động có thể nếu có xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực phục vụ công tác ứng phó, ứng cứu, khắc phục sự cố của cơ quan, đơn vị (bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có).

- Đơn vị thực hiện: Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

- Đơn vị phối hợp: Công an tỉnh; Đội UCKCSC; Nhà thầu cung cấp dịch vụ an toàn thông tin mạng (nếu có) và các đơn vị liên quan.

- Thời gian thực hiện: Cơ quan chủ quản hệ thống thông tin tự chủ trì đánh giá, kiểm tra hệ thống thông tin định kỳ 06 tháng *(trước ngày 10 tháng 6)*, 01 năm *(trước ngày 05 tháng 12)*.

f) Xây dựng phương án ứng phó, ứng cứu đối với một số tình huống sự cố cụ thể

- Nội dung thực hiện:

+ Đối với mỗi hệ thống thông tin và chương trình ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án ứng phó, ứng cứu sự cố tương ứng.

+ Trong phương án ứng phó, ứng cứu phải đặt ra được các tiêu chí phù hợp để có thể nhanh chóng xác định đúng tính chất, mức độ nghiêm trọng của sự cố khi sự cố xảy ra. Các cơ quan quản lý, vận hành hệ thống thông tin, chương trình ứng dụng phải xây dựng phương án ứng phó, ứng cứu sự cố theo hướng dẫn của các cơ quan chuyên môn cấp trên.

- Đơn vị thực hiện: Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

- Đơn vị phối hợp: Công an tỉnh; Đội UCKCSC; Các đơn vị nghiệp vụ của Bộ Công an và các đơn vị liên quan.

- Thời gian thực hiện: Sau khi Kế hoạch Ứng phó sự cố được UBND tỉnh ban hành.

2. Triển khai các nhiệm vụ khi có sự cố xảy ra: Thực hiện theo ***Quy trình ứng cứu, xử lý khẩn cấp sự cố tấn công mạng*** *tại* ***Phụ Lục 1*** *đính kèm*; các bước cụ thể như sau:

2.1. Báo cáo sự cố an toàn thông tin mạng

a) Đơn vị vận hành hệ thống thông tin có trách nhiệm báo cáo sự cố tới cơ quan chủ quản hệ thống, Công an tỉnh, Đội UCKCSC. Báo cáo sự cố phải được thực hiện ngay lập tức (khi phát hiện) và được duy trì trong suốt quá trình ứng cứu sự cố gồm: báo cáo ban đầu; báo cáo diễn biến tình hình; báo cáo phương án ứng cứu cụ thể; báo cáo xin ý kiến chỉ đạo, chỉ huy; báo cáo đề nghị hỗ trợ, phối hợp; báo cáo kết thúc ứng phó.

b) Hình thức báo cáo bằng công văn, fax, thư điện tử, nhắn tin đa phương tiện hoặc thông qua hệ thống báo cáo, cảnh báo sự cố trên địa bàn tỉnh (nếu có); mẫu báo cáo theo quy định về điều phối ứng cứu và hướng dẫn của Công an tỉnh.

c) Nội dung báo cáo ban đầu *theo mẫu tại* ***Phụ Lục 2*** *đính kèm.*

d) Nguyên tắc báo cáo, trao đổi thông tin trong ứng cứu sự cố:

- Đơn vị vận hành hệ thống thông tin báo cáo Chủ quản hệ thống thông tin, Công an tỉnh, Đội UCKCSC.

- Đội UCKCSC trao đổi với Chủ quản hệ thống thông tin; báo cáo Công an tỉnh.

e) Các tổ chức, cá nhân khi phát hiện dấu hiệu tấn công hoặc sự cố an toàn thông tin mạng cần nhanh chóng thông báo cho đơn vị vận hành hệ thống thông tin, cơ quan chủ quản hệ thống thông tin liên quan, Công an tỉnh, Đội UCKCSC.

2.2. Tiếp nhận, phát hiện, phân loại và xử lý ban đầu đối với sự cố an toàn thông tin mạng

a) Đội UCKCSC khi phát hiện sự cố hoặc tiếp nhận thông báo/ báo cáo sự cố

an toàn thông tin mạng trong phạm vi mình chịu trách nhiệm phải thực hiện:

- Ghi nhận, tiếp nhận thông báo, báo cáo sự cố an toàn thông tin mạng theo đúng quy trình.

- Thông báo ngay thông tin sự cố đến đơn vị quản lý, vận hành hệ thống thông tin, cơ quan chủ quản hệ thống thông tin, cơ quan chức năng liên quan và báo cáo Công an tỉnh.

- Phản hồi cho tổ chức, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố.

- Thẩm tra, xác minh và phân loại sự cố an toàn thông tin mạng để lựa chọn phương án ứng cứu phù hợp hoặc đề xuất với Công an tỉnh nếu vượt khả năng, thẩm quyền xử lý.

- Chủ động hỗ trợ đơn vị vận hành hệ thống thông tin ứng cứu, xử lý sự cố trong khả năng và trách nhiệm của mình.

- Giám sát diễn biến tình hình ứng cứu sự cố và báo cáo Công an tỉnh; đề xuất, xin ý kiến chỉ đạo trong trường hợp không thuộc thẩm quyền, phạm vi trách nhiệm của mình hoặc vượt khả năng xử lý.

- Theo dõi, tổng hợp các sự cố về an toàn thông tin mạng xảy ra trên địa bàn tỉnh báo cáo báo cáo Công an tỉnh theo định kỳ 6 tháng một lần và báo cáo đột xuất khi được yêu cầu.

b) Đơn vị vận hành hệ thống thông tin khi phát hiện hoặc nhận được thông báo sự cố đối với hệ thống thông tin do mình quản lý, phải thực hiện:

- Ghi nhận, tiếp nhận thông báo, báo cáo sự cố và tập hợp các thông tin liên quan theo đúng quy trình.

- Phản hồi cho tổ chức, cá nhân gửi thông báo, báo cáo ban đầu ngay sau khi nhận được để xác nhận về việc đã nhận được thông báo, báo cáo sự cố.

- Chủ trì, phối hợp cùng đơn vị cung cấp dịch vụ an toàn thông tin mạng (nếu có), Đội UCKCSC và các đơn vị chức năng liên quan tiến hành phân tích, xác minh, đánh giá tình hình sơ bộ, phân loại sự cố, triển khai ngay các hoạt động ứng cứu sự cố và báo cáo theo quy định.

- Báo cáo về sự cố, diễn biến tình hình ứng cứu sự cố, đề xuất hỗ trợ ứng cứu sự cố hoặc nâng cấp nghiêm trọng của sự cố (khi cần) cho chủ quản hệ thống thông tin và Công an tỉnh.

2.3. Triển khai các biện pháp ứng cứu, khắc phục, xử lý sự cố

a) Đơn vị vận hành, chủ quản hệ thống thông tin phối hợp thực hiện các biện pháp ứng cứu ban đầu:

- Xử lý nhanh ban đầu: (1) Thực hiện cách ly hệ thống (*máy chủ/ máy trạm lưu trữ dữ liệu quan trọng*) khỏi hệ thống mạng; nhanh chóng thực hiện lưu trữ dữ liệu quan trọng vào thiết bị điện tử chuyên dụng (*đã được kiểm tra chứng nhận bảo đảm an toàn thông tin mạng*); (2) Tạm dừng các ứng dụng dịch vụ quan trọng trong hệ thống mạng (*nếu cần thiết*), bảo vệ an toàn máy chủ, thiết bị lưu trữ dữ liệu chuyên dụng.

- Đánh giá ban đầu về sự cố: (1) Do lỗi nguồn điện; (2) Do lỗi đường truyền Internet; (3) Do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin; (4) Do lỗi của hệ thống (*thiết bị, phần mềm, hạ tầng kỹ thuật*); (5) Từ ảnh hưởng của thảm họa tự nhiên: cháy nổ, mưa bão, lũ lụt...; (6) Bị tấn công mạng.

b) Tiến hành các biện pháp khôi phục tạm thời:

- Căn cứ vào mục tiêu được ưu tiên trong khắc phục sự cố, đơn vị Chủ quản hệ thống thông tin phối hợp với các nhà cung cấp dịch vụ, Đội UCKCSC và các cơ quan chức năng khác tiến hành khôi phục một số hoạt động, dữ liệu hoặc kết nối cần thiết nhất để giảm thiểu thiệt hại đối với hệ thống thông tin, tránh làm ảnh hưởng đến uy tín của cơ quan chủ quản, quản lý hệ thống hoặc gây ảnh hưởng xấu tới xã hội.

- Chủ quản hệ thống thông tin phải phối hợp chặt chẽ, cung cấp đầy đủ thông tin để Công an tỉnh thực hiện giám sát, theo dõi quá trình phục hồi và diễn biến tiếp theo, ảnh hưởng trong thời gian chưa khắc phục triệt để sự cố.

- Xử lý hậu quả ban đầu: Chủ quản hệ thống thông tin cần nhanh chóng 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 Công an tỉnh.

- Ngăn chặn, xử lý các hành vi đã được phát hiện: Công an tỉnh điều phối hoặc chỉ đạo các đơn vị chức năng liên quan triển khai hỗ trợ phát hiện và xử lý các nguồn phát tán tấn công, ngăn chặn các tấn công từ bên ngoài vào hệ thống thông tin bị sự cố; yêu cầu đơn vị chủ quản, quản lý, vận hành cung cấp các thông tin, chứng cứ liên quan để kịp thời có biện pháp ngăn chặn, xác minh, xử lý.

c) Báo cáo, phối hợp với Đội UCKCSC xác định nguyên nhân sự cố:

- Tình huống sự cố do bị tấn công mạng: (1) Tấn công từ chối dịch vụ; (2) Tấn công giả mạo; (3) Tấn công sử dụng mã độc; (4) Tấn công truy cập trái phép, chiếm quyền điều khiển; (5) Tấn công thay đổi giao diện; (6) Tấn công mã hóa phần mềm, dữ liệu, thiết bị; (7) Tấn công phá hoại hệ thống thông tin, dữ liệu, phần mềm; (8) Tấn công nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu; (9) Tấn công tổng hợp sử dụng kết hợp nhiều hình thức; (10) Các hình thức tấn công mạng mới, khác.

- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống: (1) Lỗi trong cập nhật, thay đổi, cấu hình phần cứng; (2) Lỗi trong cập nhật, thay đổi, cấu hình phần mềm; (3) Lỗi liên quan đến chính sách và thủ tục an toàn thông tin; (4) Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc; (5) Lý do khác liên quan đến trách nhiệm được quy định đối với người quản trị, vận hành hệ thống.

- Tình huống sự cố do lỗi xuất phát từ người dùng cuối (*quá trình truy cập, khai thác vào hệ thống*): (1) Chia sẻ thông tin, sử dụng chung tài khoản sai quy định; (2) Làm lộ, mất thông tin tài khoản; (3) Thực hiện sai các hướng dẫn đã ban hành về quy trình, quy chế, chính sách và thủ tục an toàn thông tin người dùng.

d) Phối hợp với Đội UCKCSC triển khai, thực hiện các biện pháp ứng cứu, xử lý khắc phục sự cố:

- Xác định phạm vi đối tượng, mục tiêu cần ưu tiên ứng cứu; thực hiện ứng cứu theo thứ tự mức độ quan trọng (*thành phần chức năng, ứng dụng dịch vụ, dữ liệu*

quan trọng cần bảo vệ, khôi phục).

- Tìm hiểu về các sự cố tương tự, có liên quan đã xảy ra, phân tích, tìm giải pháp ứng cứu, xử lý khắc phục hiệu quả nhất.

- Phân loại, thực hiện ứng cứu mục tiêu: khôi phục hoạt động, bảo đảm bí mật dữ liệu (*bảo đảm tính toàn vẹn dữ liệu, hạn chế mức thấp nhất mức độ thất thoát dữ liệu*).

- 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.

- Nhận định diễn biến tình hình và phương thức thủ đoạn tấn công (nếu có), dự đoán các diễn biến tiếp theo có thể xảy ra; xây dựng phương án, xác định biện pháp ngăn chặn tấn công mạng, hướng đến việc thực hiện xác minh thông tin, truy vết đối tượng tấn công.

- Cảnh báo sự cố trên mạng lưới ứng cứu của tỉnh, các đơn vị có liên quan, kịp thời phòng tránh xảy ra các sự cố tương tự.

e) Một số biện pháp xử lý, khắc phục sự cố khẩn cấp:

- Khắc phục sự cố, gỡ bỏ mã độc: (1) Sao lưu hệ thống trước và sau khi xử lý sự cố; (2) Tiêu diệt các mã độc, phần mềm độc hại; (3) Khôi phục hệ thống, dữ liệu và kết nối; (4) Cấu hình hệ thống an toàn; (5) Kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố; (6) Khắc phục các điểm yếu an toàn thông tin; (7) Bổ sung các thiết bị, phần cứng, phần mềm bảo vệ an toàn thông tin cho hệ thống; (8) Triển khai theo dõi, giám sát, ngăn chặn khả năng lặp lại sự cố hoặc xảy ra các sự cố tương tự; (9) Tiêu diệt các mã độc, phần mềm độc hại; (10) Khôi phục hệ thống, dữ liệu và kết nối; (11) Cấu hình hệ thống an toàn; (12) Kiểm tra thử toàn bộ hệ thống sau khi khắc phục sự cố; (13) Khắc phục các điểm yếu an toàn thông tin hệ thống; (14) Bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin cho hệ thống; (15) Triển khai theo dõi, giám sát, ngăn chặn khả năng lặp lại sự cố hoặc xảy ra các sự cố tương tự.

- Ngăn chặn, xử lý hậu quả: Chủ quản hệ thống thông tin có trách nhiệm xử lý các hậu quả do sự cố hệ thống thông tin của mình gây ra ảnh hưởng đến người dân, cơ quan, tổ chức khác. Các đơn vị thuộc thành phần tham gia tác nghiệp ứng cứu khẩn cấp, dựa trên các kết quả phân tích, điều tra, sử dụng các nguồn lực, phương tiện và nghiệp vụ của mình để tiến hành ngăn chặn các hành vi gây ra sự cố và hỗ trợ xử lý, khắc phục hậu quả.

f) Xác minh nguyên nhân và truy tìm nguồn gốc: các đơn vị tham gia tác nghiệp ứng cứu khẩn cấp sau khi 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 xác minh và truy tìm nguồn gốc báo cáo Công an tỉnh - Cơ quan Thường trực Tiểu ban An toàn an ninh mạng, nội dung cụ thể: (1) Đối tượng bị tấn công mạng; (2) Phương thức thủ đoạn tấn công (*quy trình, kỹ thuật, loại mã độc, phần mềm độc hại*); (3) Thời gian tấn công; (4) Các thiệt hại đã xảy ra; (5) Đối tượng tấn công mạng; (6) Dự đoán khả năng xảy ra các tấn công tương tự và thiệt hại.

g) Đánh giá kết quả triển khai phương án ứng cứu sự cố khẩn cấp, bảo đảm an toàn thông tin mạng: Công an tỉnh tổng hợp toàn bộ các báo cáo phân tích có liên

quan đến triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng để báo cáo với Bộ Công an; phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung cho các sự cố tương tự.

h) Tổng kết: Đơn vị chủ trì, Công an tỉnh phối hợp với đơn vị chủ quản hệ thống thông tin, các đơn vị thuộc Bộ phận tác nghiệp ứng cứu khẩn cấp căn cứ kết quả đánh giá của Bộ Công an sẽ thực hiện hoàn tất các nhiệm vụ sau, kết thúc hoạt động ứng cứu sự cố khẩn cấp để thực hiện việc lưu hồ sơ, tài liệu lưu trữ và 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 sự cố tương tự. Các đơn vị tham gia vào hoạt động ứng cứu sự cố thực hiện tổng kết, báo cáo toàn diện sự cố (*thực hiện theo mẫu tại **Phụ Lục 3** đính kèm*) cho cơ quan cấp trên, tổ chức họp báo hoặc gửi thông tin cho truyền thông nếu cần thiết.

3. Phương án ứng phó, ứng cứu đối với một số tình huống cụ thể

a) Đối với mỗi hệ thống thông tin, chương trình ứng dụng, cần xây dựng tình huống, kịch bản sự cố cụ thể và đưa ra phương án ứng phó, ứng cứu sự cố tương ứng. Việc xây dựng phương án ứng phó, ứng cứu sự cố cần đảm bảo các nội dung sau:

- Quy trình triển khai và các bước ưu tiên ứng cứu ban đầu khi hệ thống thông tin gặp sự cố, có phân theo các loại sự cố.

- Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân và nguồn gốc xảy ra sự cố nhằm áp dụng phương án ứng phó, ứng cứu, khắc phục sự cố bảo đảm yếu tố phù hợp, hiệu quả:

+ Sự cố do bị tấn công mạng.

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

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

+ Sự cố liên quan đến các thiên tai, thảm họa tự nhiên như bão, lũ lụt, động đất, hỏa hoạn...

b) Phương án ứng phó, ứng cứu, khắc phục, xử lý sự cố đối với một hoặc nhiều tình huống sau:

- Tình huống sự cố do bị tấn công mạng:

+ Tấn công từ chối dịch vụ.

+ Tấn công giả mạo.

+ Tấn công sử dụng mã độc.

+ Tấn công truy cập trái phép, chiếm quyền điều khiển.

+ Tấn công thay đổi giao diện.

+ Tấn công mã hóa phần mềm, dữ liệu, thiết bị.

+ Tấn công phá hoại thông tin, dữ liệu, phần mềm.

+ Tấn công 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 mạng khác.

- Tình huống sự cố do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật

+ Sự cố nguồn điện.

+ Sự cố đường kết nối Internet.

+ Sự cố do lỗi phần mềm, phần cứng, ứng dụng của hệ thống thông tin.

+ Sự cố liên quan đến quá tải hệ thống.

+ Sự cố khác do lỗi của hệ thống, thiết bị, phần mềm, hạ tầng kỹ thuật.

- Tình huống sự cố do lỗi của người quản trị, vận hành hệ thống

+ Lỗi trong cập nhật, thay đổi, cấu hình phần cứng.

+ Lỗi trong cập nhật, thay đổi, cấu hình phần mềm.

+ Lỗi liên quan đến chính sách và thủ tục an toàn thông tin.

+ Lỗi liên quan đến việc dừng dịch vụ vì lý do bắt buộc.

+ Lỗi khác liên quan đến người quản trị, vận hành hệ thống.

- Tình huống sự cố liên quan đến các thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn...

c) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, giữa các tổ chức trong ứng phó, ngăn chặn, ứng cứu, khắc phục sự cố.

d) Phương án về nhân lực, trang thiết bị, giải pháp phần mềm, phương tiện, công cụ và dự kiến kinh phí để thực hiện, ứng phó, ứng cứu, xử lý đối với từng tình huống sự cố cụ thể.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch này được bố trí từ nguồn ngân sách hàng năm của tỉnh.

IV. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh, các sở, ban, ngành; UBND các địa phương

- Giám đốc Công an tỉnh, Thủ trưởng các sở, ban, ngành, Chủ tịch UBND các địa phương căn cứ nội dung Kế hoạch này và tình hình thực tế ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng của cơ quan, đơn vị, địa phương năm 2025 bảo đảm đúng tiến độ, chất lượng, hiệu quả và tiết kiệm, tránh hình thức, lãng phí.

- Xây dựng nội dung, dự toán kinh phí lồng ghép trong Kế hoạch chuyển đổi số hàng năm của cơ quan, đơn vị, địa phương để triển khai các nhiệm vụ được giao tại Kế hoạch này.

- Phân công lãnh đạo phụ trách an toàn thông tin và thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về an toàn thông tin mạng của cơ quan, đơn vị.

- Thực hiện bố trí cán bộ, công chức chuyên trách về an toàn thông tin mạng tại cơ quan, đơn vị, địa phương; kịp thời thông báo về Công an tỉnh khi có sự thay đổi cán bộ, công chức chuyên trách về an toàn thông tin mạng tại cơ quan, đơn vị, địa phương hoặc cán bộ, công chức, viên chức đang là thành viên tham gia Đội UCKCSC.

- Thực hiện xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông

tin theo quy định tại Điều 13, Điều 14 và Điều 15 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ và theo hướng dẫn tại Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Thực hiện việc xác định cấp độ và xây dựng hồ sơ đề xuất cấp độ an toàn thông tin đối với hệ thống thông tin có sử dụng camera giám sát theo Chỉ thị 23/CT-TTg ngày 26/12/2022 của Thủ tướng Chính phủ về tăng cường công tác bảo đảm an toàn thông tin mạng, an ninh thông tin cho thiết bị camera giám sát và hướng dẫn tại Công văn số 294/CATTT-ATHTTT ngày 13/3/2023 của Cục An toàn thông tin (Bộ Thông tin và Truyền thông) về việc hướng dẫn bảo đảm an toàn hệ thống thông tin đối với các hệ thống thông tin có sử dụng camera giám sát, gửi về Công an tỉnh thẩm định.

- Cử cán bộ tham gia các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn về bảo đảm an toàn thông tin mạng để nâng cao kỹ năng và công tác tham mưu, triển khai giám sát, bảo đảm an toàn thông tin.

- Tích cực phối hợp với cơ quan, đơn vị chủ trì thực hiện các nhiệm vụ được giao theo Kế hoạch này.

2. Công an tỉnh - Cơ quan Thường trực Tiểu ban An toàn An ninh mạng

Là cơ quan đầu mối, chuyên trách về ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh, có trách nhiệm xây dựng và triển khai Kế hoạch này; tổ chức theo dõi, đôn đốc, phối hợp với các sở, ban, ngành, địa phương trong việc triển khai thực hiện Kế hoạch này; báo cáo kết quả thực hiện về UBND tỉnh để theo dõi và chỉ đạo.

- Nghiên cứu, cập nhật các kỹ năng, phương pháp, biện pháp kỹ thuật về quản lý, theo dõi, ứng phó, xử lý sự cố về an toàn thông tin mạng; hướng dẫn các đơn vị chủ quản, quản lý, vận hành các hệ thống thông tin quan trọng thực hiện đúng, đầy đủ các nội dung liên quan đến bảo đảm an toàn thông tin, kịp thời xử lý và giảm thiểu rủi ro, thiệt hại khi sự cố xảy ra.

3. Sở Khoa học và Công nghệ

Nghiên cứu, cập nhật các giải pháp quản lý, vận hành hệ thống thông tin tại Trung tâm Dữ liệu tỉnh hiệu quả, tập trung theo dõi, kịp thời hướng dẫn các đơn vị truy cập, khai thác các hệ thống thông tin dùng chung của tỉnh bảo đảm đúng quy định, đạt hiệu quả; ban hành, sửa đổi, bổ sung các quy chế, quy trình khai thác vào hệ thống; chủ động phối hợp với Công an tỉnh thường xuyên giám sát, kịp thời phát hiện, xử lý khắc phục các điểm yếu, lỗ hổng bảo mật hệ thống và thực hiện các biện pháp phòng chống, ngăn chặn tấn công mạng, bảo đảm hệ thống thông tin vận hành thông suốt, ổn định, đáp ứng yêu cầu quá trình chuyển đổi số phải song hành với thực hiện tốt công tác bảo đảm an toàn thông tin mạng.

4. Sở Tài chính

Trên cơ sở dự toán kinh phí cho công tác ứng phó sự cố, bảo đảm an toàn thông tin mạng do Công an tỉnh tổng hợp trong Kế hoạch chuyển đổi số hàng năm của tỉnh, Sở Tài chính xem xét, cân đối theo khả năng ngân sách để tham mưu trình

cấp thẩm quyền bố trí kinh phí từ nguồn vốn sự nghiệp, nguồn vốn đầu tư cho các cơ quan, đơn vị thuộc tỉnh được giao nhiệm vụ thực hiện theo đúng quy định.

Trong quá trình thực hiện nếu phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương kịp thời phối hợp với Công an tỉnh để tổng hợp, hướng dẫn xử lý theo thẩm quyền hoặc báo cáo, tham mưu UBND tỉnh xem xét giải quyết theo đúng quy định pháp luật.

(Đính kèm phụ lục 1, phụ lục 2, phụ lục 3)./.

Nơi nhận:
- Bộ Công an (báo cáo);
- Thường trựcTỉnh ủy (báo cáo);
- Thường trực HĐND tỉnh (báo cáo);
- Chủ tịch và các PCTUBND tỉnh;
- Thường trực UBMTTQVN tỉnh;
- Các sở, ban, ngành;
- UBND các huyện, thị xã, thành phố;
- Các đoàn thể chính trị - xã hội;
- Văn phòng UBND tỉnh;
- Lưu: VT, NL, NgM. Các Phòng chuyên môn.

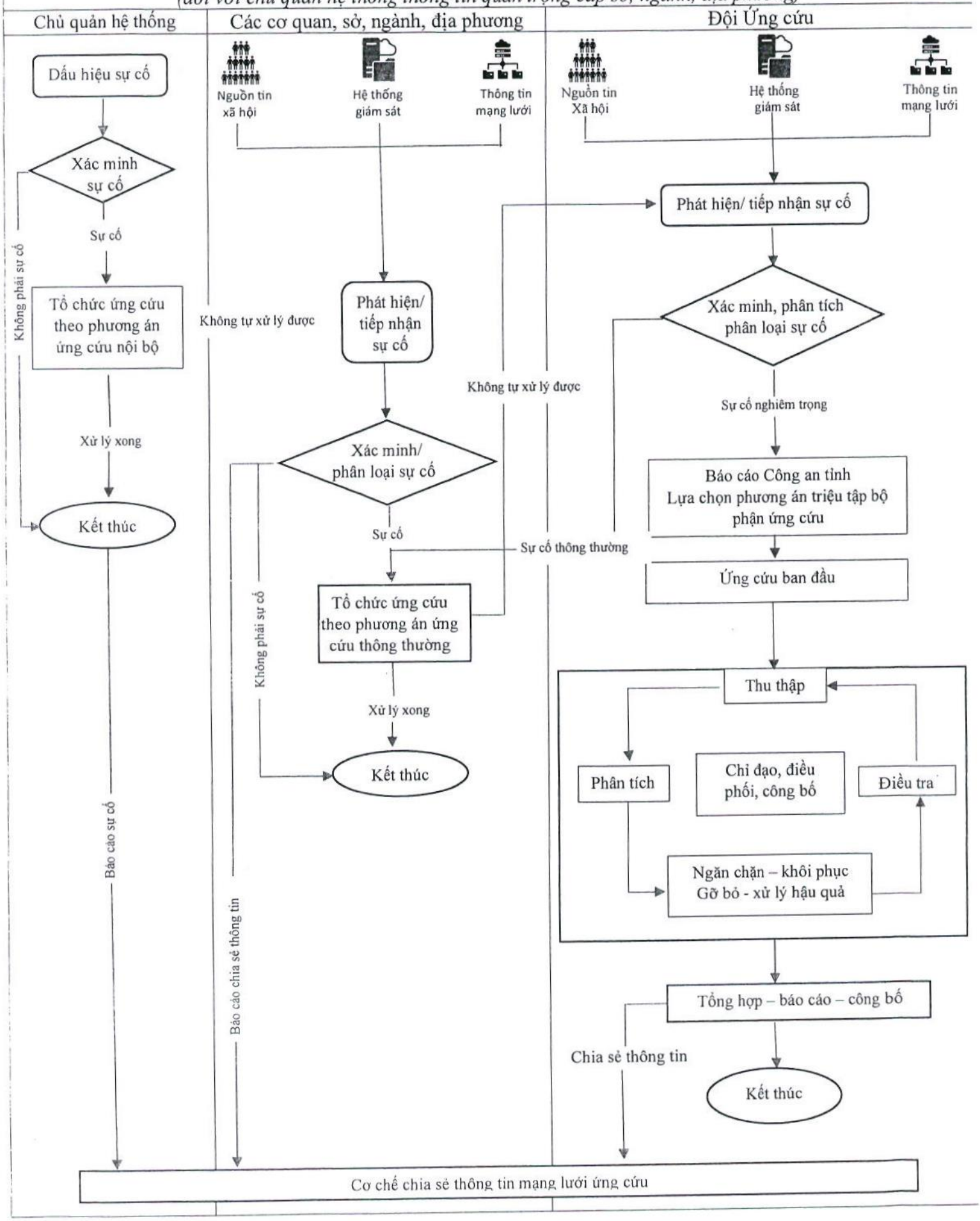
TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Tấn Tuân

Phụ Lục 1

Quy trình tổng thể hệ thống phương án ứng cứu sự cố an toàn thông tin mạng

(đối với chủ quản hệ thống thông tin quan trọng cấp sở, ngành, địa phương)



Phụ Lục 2

Báo cáo ban đầu sự cố an toàn thông tin mạng của Hệ thống thông tin (HTTT)

I. Thông tin về tổ chức/ cá nhân báo cáo sự cố

1. Tên tổ chức/ cá nhân báo cáo sự cố (*)[1] .....

2. Địa chỉ (*): .....

3. Điện thoại (*).....; Email (*)[2]:.....

II. Người liên hệ

1. Họ tên (*).....; Chức vụ:.....

2. Điện thoại (*):.....; Email (*).....

III. Thông tin chi tiết về hệ thống bị sự cố

Tên đơn vị đang quản lý, vận hành hệ HTTT (*)	*Điền tên đơn vị quản lý, vận hành hoặc được thuê quản lý, vận hành hệ thống thông tin*				
Cơ quan chủ quản HTTT	*Điền tên cơ quan chủ quản*				
Tên HTTT xảy ra sự cố	*Điền tên hệ thống bị sự cố, tên miền, địa chỉ IP liên quan*				
Phân loại cấp độ HTTT	☐ 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	*Điền tên nhà cung cấp dịch vụ an toàn thông tin*				
Tên nhà cung cấp dịch vụ kết nối bên ngoài	*Điền tên nhà cung cấp dịch vụ kết nối bên ngoài (nếu có)*				
Dải IP Public kết nối hệ thống bên ngoài	*Điền thông tin dải IP công khai kết nối với hệ thống ra bên ngoài*				

IV. 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 cuộc tấn công đã xảy ra chưa và bất kỳ các nguy cơ dẫn đến khả năng phá hoại hoặc gián đoạn dịch vụ. Xác định mức độ nhạy cảm của thông tin liên quan hoặc những đối tượng bị ảnh hưởng bởi sự cố: .....

.....

.....

.....

1. Ngày phát hiện sự cố (*) (dd/mm/yyyy): .....

2. Thời gian phát hiện sự cố (*).....giờ.....phút.....giây.....

3. Hiện trạng sự cố (*):

☐ Đã được xử lý ☐ Chưa được xử lý

---

[1] Các mục có dấu (*) là nội dung bắt buộc điền thông tin.

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

4. Cách thức phát hiện (*):

☐ Qua hệ thống phát hiện xâm nhập ☐ Kiểm tra dữ liệu lưu lại (log file)

☐ Nhận được thông báo từ .....

☐ Nội dung khác .....

5. Đã gửi thông báo sự cố cho (*):

☐ Thành viên Đội UPKCSC ☐ Công an tỉnh

☐ Đơn vị xây dựng, phát triển hệ thống, dịch vụ, cổng/ trang thông tin điện tử.....

☐ Cơ quan chức năng có liên quan khác .....

6. Thông tin bổ sung về hệ thống xảy ra sự cố:

a) Hệ điều hành:.....; Phiên bản:.....

b) Các dịch vụ có trên hệ thống: (*đánh dấu những dịch vụ có trên hệ thống*)

☐ Web Server ☐ Mail Server ☐ Database Server

☐ Dịch vụ khác .....

c) Các giải pháp an toàn thông tin đã triển khai: (*đánh dấu những giải pháp)*

☐ Antivirus ☐ Firewall ☐ Phòng chống xâm nhập

☐ Giải pháp khác .....

d) Các địa chỉ IP của hệ thống:.....

.....

e) Các tên miền của hệ thống:.....

.....

f) Mục đích chính của hệ thống:.....

.....

g) Thông tin gửi kèm: (*đánh dấu những dịch vụ có trên hệ thống*)

☐ Nhật ký hệ thống ☐ Mẫu virus, mã độc ☐ Danh sách IP

☐ Thông tin khác .....

h) Thông tin cung cấp trong thông báo sự cố này phải giữ bí mật: ☐ Có; ☐ Không

IV. Kiến nghị, đề xuất hỗ trợ

Mô tả tóm lược về kiến nghị, đề xuất được hỗ trợ (nếu có).....

.....

.....

.....

.....

V. Thời gian thực hiện báo cáo sự cố (*): .../.../.../.../...(*ngày/tháng/năm/giờ/phút*)

CÁ NHÂN/ ĐẠI DIỆN THEO PHÁP LUẬT

(*Ký tên, dóng dấu*)

Phụ Lục 3

Báo cáo kết thúc ứng phó sự cố an toàn thông tin mạng

I. Thông tin về tổ chức/ cá nhân báo cáo sự cố

1. Tên tổ chức/ cá nhân báo cáo sự cố (*)[1] .....

2. Địa chỉ (*): .....

3. Điện thoại (*).....; Email (*)[2]:.....

II. Ký hiệu báo cáo ban đầu sự cố: Số ký hiệu/ Ngày báo cáo (dd/mm/yyyy):.....

III. Thông tin chi tiết về hệ thống bị sự cố

Tên đơn vị đang quản lý, vận hành HTTT (*)	*Điền tên đơn vị quản lý, vận hành hoặc được thuê quản lý, vận hành hệ thống thông tin*				
Cơ quan chủ quản HTTT	*Điền tên cơ quan chủ quản*				
Tên HTTT xảy ra sự cố	*Điền tên hệ thống bị sự cố, tên miền, địa chỉ IP liên quan*				
Phân loại cấp độ HTTT	☐ Cấp độ 1	☐ Cấp độ 2	☐ Cấp độ 3	☐ Cấp độ 4	☐ Cấp độ 5

IV. Tên/ Mô tả sơ bộ về sự cố

Tóm tắt ngắn gọn về sự cố, diễn biến mức độ, phạm vi ảnh hưởng.....

.....

.....

.....

1. Ngày phát hiện sự cố (*) (dd/mm/yyyy): .....

2. Thời gian phát hiện sự cố (*).....giờ.....phút.....giây.....

V. Các tài liệu đính kèm

Liệt kê, thống kê các tài liệu, báo cáo liên quan (tập tin, văn bản, hình ảnh, phương án xử lý, log file) .....

.....

.....

.....

CÁ NHÂN/ ĐẠI DIỆN THEO PHÁP LUẬT

(Ký tên, đóng dấu)

---

[1] Các mục có dấu (*) là nội dung bắt buộc điền thông tin.

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