ỦY BAN NHÂN DÂN TỈNH THANH HÓA	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 150 /KH-UBND	*Thanh Hóa, ngày 19 tháng 5 năm 2026*

KẾ HOẠCH
Ứng cứu sự cố, bảo đảm an toàn, an ninh mạng trên địa bàn tỉnh Thanh Hoá

Thực hiện các văn bản quy phạm pháp luật[1]; chỉ đạo của Chính phủ[2]; hướng dẫn của các bộ, ngành trung ương đối với công tác bảo đảm an toàn thông tin mạng[3], UBND tỉnh Thanh Hoá ban hành Kế hoạch ứng cứu sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Thanh Hoá, 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 kịp thời, 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 bảo mật 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 chuyển đổi số, xây dựng chính quyền 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

---

[1] Luật Công nghệ thông tin số 67/2006/QH11 ngày 29/6/2006; Luật An toàn thông tin mạng số 86/2015/QH13 ngày 19/11/2015; Luật An ninh mạng số 116/2025/QH15 ngày 10/12/2025; 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; 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 964/QĐ-TTg ngày 10/8/2022 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 đến năm 2025, tầm nhìn 2030; 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; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của 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.

[2] Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng chống phần mềm độc hại; Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Chỉ thị số 09/CT-TTg ngày 23/02/2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ.

[3] Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ trưởng Bộ Thông tin và Truyền thông về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng.

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.

2. Yêu cầu

- Ứng cứu sự cố trước hết phải thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của đơn vị vận hành hệ thống thông tin. Chủ động, kịp thời, nhanh chóng, chính xác, đồng bộ và hiệu quả; phối hợp chặt chẽ, đồng bộ và hiệu quả giữa các cơ quan, đơn vị, tổ chức, cá nhân. Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an toàn thông tin mạng.

- Lực lượng ứng cứu sự cố an toàn thông tin mạng tham gia thường xuyên, đầy đủ các chương trình diễn tập tình huống hoặc thực chiến về ứng cứu sự cố an toàn thông tin mạng do các cơ quan chuyên trách tổ chức. Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác bảo đảm an toàn thông tin giữa các cơ quan, doanh nghiệp nhà nước trên địa bàn tỉnh; tận dụng sự phối hợp, hỗ trợ của các đơn vị nghiệp vụ của Bộ Công an và cơ quan điều phối quốc gia về ứng cứu sự cố (VNCERT).

- Hoạt động ứng cứu sự cố an toàn thông tin mạng phải chuyển từ bị động sang chủ động, bao gồm: Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý. 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.

- Bảo đảm các nguồn lực (nhân lực, kinh phí) 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.

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; tập huấn, nâng cao nhận thức, kỹ năng về an toàn thông tin mạng

- Nội dung thực hiện:

+ Tổ chức tuyên truyền, phổ biến, hướng dẫn nội dung của Luật An ninh mạng số 116/2025/QH15 và các quy định về công tác ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng.

+ Tập huấn nâng cao nhận thức, kỹ năng về an ninh mạng cho cán bộ, công chức, viên chức, người lao động.

- Đơn vị chủ trì: Công an tỉnh.

- Đơn vị phối hợp: Các sở, ban, ngành, đơn vị cấp tỉnh, UBND các xã, phường và các đơn vị liên quan.

- Thời gian thực hiện: Hằng năm.

b) Triển khai các chương trình diễn tập[4], 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 cứu 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 chủ trì: Công an tỉnh.

- 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 có liên quan.

- Thời gian thực hiện: Hằng năm.

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

- Nội dung thực hiện:

+ Xây dựng, mở rộng hệ thống Giám sát an ninh mạng (SOC) thực hiện giám sát, bảo đảm an toàn thông tin mạng cho toàn bộ các cơ quan trong hệ thống chính trị tại địa phương, kết nối Trung tâm an ninh mạng quốc gia.

+ Tiếp tục sử dụng, vận hành hệ thống Giám sát an toàn thông tin mạng trước đây của tỉnh; 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.

+ Kiểm tra, đánh giá thực tế công tác ứng cứu sự cố, công tác bảo đảm an ninh mạng, an toàn thông tin tại các cơ quan, đơn vị. Hỗ trợ, hướng dẫn nghiệp vụ ứng cứu, xử lý sự cố an toàn thông tin mạng tại các hệ thống thông tin và ứng dụng các hệ thống phần mềm dùng chung tại các ngành, địa phương trên địa bàn tỉnh.

+ 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.

+ Triển khai kiểm tra, đánh giá, rà soát các lỗ hổng bảo mật, an toàn thông tin và đánh giá mức độ an toàn thông tin của Cổng/trang thông tin điện tử của các cơ quan, tổ chức trên địa bàn tỉnh.

- Đơn vị chủ trì: Công an tỉnh.

---

[4] Thực hiện theo Quy định tại Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và Truyền thông.

- Đơn vị phối hợp: Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Thanh Hoá *(sau đây gọi tắt là Đội UCSC)*; Đơn vị chủ quản, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

- Thời gian thực hiện: Thường xuyên.

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 UCSC; 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 chủ trì: Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, địa phương).

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

- Thời gian thực hiện: Hằng 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).

+ Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng bảo mật đối với các hệ thống thông tin thuộc phạm vi quản lý; khắc phục lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng[5].

+ 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 địa bàn tỉnh.

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

- Đơn vị phối hợp: Công an tỉnh; Đội UCSC; Sở Khoa học và Công nghệ;

[5] Thực hiện theo quy định tại Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ.

nhà thầu cung cấp dịch vụ an toàn thông tin mạng (nếu có) và các đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên (tối thiểu 06 tháng/01 lần).

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

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

- Thời gian thực hiện: Thường xuyên.

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 an toàn thông tin mạng tại Phụ lục 1 đính kèm)*, các bước cụ thể như sau:

a) Báo cáo sự cố an toàn thông tin mạng[6]

- Đơn vị vận hành hệ thống thông tin có trách nhiệm báo cáo sự cố tới cơ quan chủ quản hệ thống thông tin, Công an tỉnh, Đội UCSC, Cơ quan điều phối quốc gia *(Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam -VNCERT, địa chỉ: Toà nhà Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao, Lô E2, KĐT Cầu Giấy, phường Cầu Giấy, thành phố Hà Nội, Website: www.vncert.vn)*. 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.

- 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.

[6] Quy định tại Điều 11 Quyết định số 05/2017/QĐ-TTg 16/3/2017 của Thủ tướng Chính phủ; Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông.

- Nội dung báo cáo ban đầu theo mẫu tại Phụ lục 2 đính kèm.

- 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 UCSC, Cơ quan điều phối quốc gia.

+ Đội UCSC trao đổi với Chủ quản hệ thống thông tin; báo cáo Công an tỉnh và Cơ quan điều phối quốc gia.

- 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 để báo cáo đến cơ quan chủ quản hệ thống thông tin, Công an tỉnh, Đội UCSC.

b) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu đối với sự cố an toàn thông tin mạng[7]

- Đội UCSC 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 Cơ quan điều phối quốc gia, 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[8] 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 Công an tỉnh theo định kỳ 6 tháng một lần và báo cáo đột xuất khi được yêu cầu.

- 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

---

[7] Quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg 16/3/2017 của Thủ tướng Chính phủ; Điều 10 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông.

[8] Quy định tại Điều 9 Quyết định số 05/2017/QĐ-TTg 16/3/2017 của Thủ tướng Chính phủ.

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 UCSC 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.

- Công an tỉnh sau khi nhận được báo cáo về sự cố an toàn thông tin mạng cần thực hiện:

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

+ Chủ động hỗ trợ đơn vị chủ quản, vận hành hệ thống thông tin ứng cứu, xử lý sự cố trong khả năng và trách nhiệm của mình. Nếu vượt quá khả năng xử lý, báo cáo Cơ quan điều phối quốc gia để xin ý kiến xử lý.

+ Giám sát, theo dõi tình hình ứng cứu sự cố, thu thập dấu vết, chứng cứ số phục vụ xử lý sự cố ban đầu và công tác đấu tranh phòng, chống tội phạm sử dụng công nghệ cao.

- Chủ quản hệ thống thông tin phối hợp, tạo mọi điều kiện thuận lợi cho Công an tỉnh, Đội UCSC và các đơn vị chức năng có liên quan thực hiện ứng cứu sự cố an toàn thông tin mạng kịp thời, đạt hiệu quả.

c) Triển khai các biện pháp ứng cứu, khắc phục, xử lý sự cố[9]

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;

---

[9] Quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg 16/3/2017 của Thủ tướng Chính phủ; Điều 11 Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông.

(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;

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

- Tiến hành các biện pháp khôi phục tạm thời:

+ Căn cứ vào mục tiêu được ưu tiên trong khắc phục sự cố, Chủ quản hệ thống thông tin phối hợp với các nhà cung cấp dịch vụ, Đội UCSC 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.

- Báo cáo, phối hợp với Đội UCSC 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.

- Phối hợp với Đội UCSC 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, an toàn dữ liệu, hạn chế 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.

- 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.

3. Triển khai nhiệm vụ sau khi kết thúc ứng cứu sự cố

a) 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.

b) 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, truy tìm nguồn gốc để báo cáo Công an tỉnh - Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh, 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.

c) 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 và trao đổi với các đơn vị chức năng có liên quan; 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.

d) Tổng kết:

- Công an tỉnh, Đội UCSC 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, 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 *(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.

- Hằng năm, tổ chức tổng kết hoạt động của Đội UCSC.

III. ĐIỀU KIỆN ĐẢM BẢO

1. Lực lượng tham gia ứng cứu sự cố

- Chủ quản hệ thống thông tin; đơn vị quản lý, vận hành hệ thống thông tin.

- Các sở, ban, ngành, đơn vị, đoàn thể cấp tỉnh; UBND các xã, phường; các cơ quan, đơn vị.

- Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Thanh Hoá.

- Doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng trên địa bàn tỉnh.

- Mời các cơ quan chuyên trách của các bộ, ngành có chức năng ứng cứu sự cố an ninh mạng, an toàn thông tin cùng tham gia.

2. Kinh phí

- Kinh phí thực hiện Kế hoạch này được bố trí từ nguồn ngân sách hằng năm của tỉnh cho hoạt động ứng cứu sự cố, bảo đảm an ninh mạng, an toàn thông tin và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

- Chủ quản hệ thống thông tin bố trí kinh phí để thực hiện Kế hoạch, phương án ứng cứu sự cố, dự phòng kinh phí xử lý sự cố, khắc phục hậu quả, khôi phục dữ liệu và hoạt động bình thường của hệ thống thông tin của mình.

IV. PHÂN CÔNG NHIỆM VỤ

1. Các sở, ban, ngành, đơn vị cấp tỉnh và UBND các xã, phường

- Giám đốc các sở, Thủ trưởng các ban, ngành, đơn vị cấp tỉnh, Chủ tịch UBND các xã, phường căn cứ nội dung Kế hoạch này và tình hình thực tế để ban hành Kế hoạch ứng cứu sự cố, bảo đảm an toàn thông tin mạng của cơ quan, đơn

vị, địa phương bảo đảm đúng tiến độ, chất lượng, hiệu quả và tiết kiệm, tránh hình thức, lãng phí.

- Ưu tiên bố trí nguồn lực *(nhân lực, kinh phí)* và điều kiện để triển khai hoạt động ứng cứu sự cố an ninh mạng, an toàn thông tin trong hoạt động nội bộ của cơ quan, tổ chức, lĩnh vực quản lý. Xây dựng nội dung, dự toán kinh phí lồng ghép trong Kế hoạch chuyển đổi số hằng 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 trong phạm vi lĩnh vực quản lý.

- Phân công lãnh đạo, cán bộ tham gia Đội ứng cứu sự cố an ninh mạng của tỉnh theo yêu cầu.

- 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 UCSC.

- 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 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 ninh, an toàn 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.

- Tổ chức rà soát, đánh giá tổng thể về an ninh mạng, bảo mật thông tin, an toàn dữ liệu đối với hệ thống thông tin thuộc phạm vi quản lý, đề xuất giải pháp bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu. Phối hợp với các đơn vị chức năng khắc phục ngay tình trạng "nợ tuân thủ" các điều kiện đảm bảo an ninh, an toàn thông tin.

- 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 ninh mạng

- Tham mưu cho Chủ tịch UBND tỉnh ban hành Quyết định thành lập, kiện toàn Đội ứng cứu khẩn cấp sự cố bảo đảm an toàn thông tin mạng của tỉnh.

- 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.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát công tác đảm bảo an toàn thông tin hằng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước trong tỉnh.

- Xây dựng và vận hành cơ chế cảnh báo sớm về nguy cơ, sự cố an toàn thông tin mạng; kịp thời kiến nghị biện pháp phòng ngừa đến các cơ quan, đơn vị trên địa bàn tỉnh.

- Chủ trì, phối hợp thực hiện điều tra, xác minh, truy vết nguồn gốc các cuộc tấn công mạng; thu thập; phân tích chứng cứ số phục vụ xử lý sự cố và đấu tranh phòng, chống tội phạm sử dụng công nghệ cao theo quy định của pháp luật.

- Theo dõi, hướng dẫn, kiểm tra, giám sát việc thực hiện ứng phó sự cố đảm bảo an toàn thông tin tại các sở, ban, ngành, UBND các xã, phường.

- Định kỳ (06 tháng, 01 năm) hoặc đột xuất, tổng hợp báo cáo kết quả thực hiện ứng phó sự cố, đảm bảo an ninh mạng, an toàn thông tin trên địa bàn tỉnh để báo cáo UBND tỉnh và Bộ Công an.

- 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.

- Phối hợp với các đơn vị liên quan tổ chức tuyên truyền các hoạt động ứng phó sự cố, bảo đảm an ninh mạng, an toàn thông tin trên các trang/cổng thông tin điện tử của tỉnh, các fanpage, blog, diễn đàn,...

- Nghiên cứu, thiết lập kênh hotline 24/7 hỗ trợ ứng cứu sự cố an ninh mạng trên nền tảng ứng dụng bảo mật (Signet); hướng dẫn thành viên Đội UCSC của tỉnh tham gia.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho hoạt động của Đội UCSC của tỉnh.

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, thường xuyên kiểm tra, 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 ninh, an toàn thông tin.

- Nghiên cứu, đề xuất các giải pháp, ứng dụng khoa học công nghệ phục vụ công tác đảm bảo, ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh.

- Cử cán bộ có trình độ, kinh nghiệm tham gia xử lý, ứng cứu các sự cố về an toàn thông tin, an ninh mạng xảy ra trên địa bàn tỉnh khi có yêu cầu của cơ quan, đơn vị chức năng.

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 có 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.

V. TỔ CHỨC THỰC HIỆN

Kế hoạch này thay thế Kế hoạch số 139/KH-UBND ngày 17/7/2018 của UBND tỉnh về ứng phó sự cố đảm bảo an toàn thông tin mạng trên địa bàn tỉnh Thanh Hoá.

Các sở, ban, ngành, đoàn thể của tỉnh; UBND các xã, phường; các cơ quan, đơn vị, doanh nghiệp có liên quan căn cứ nội dung Kế hoạch này và tình hình thực tế ban hành Kế hoạch ứng cứu sự cố, bảo đảm an toàn thông tin của cơ quan và tổ chức triển khai, thực hiện nghiêm túc.

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

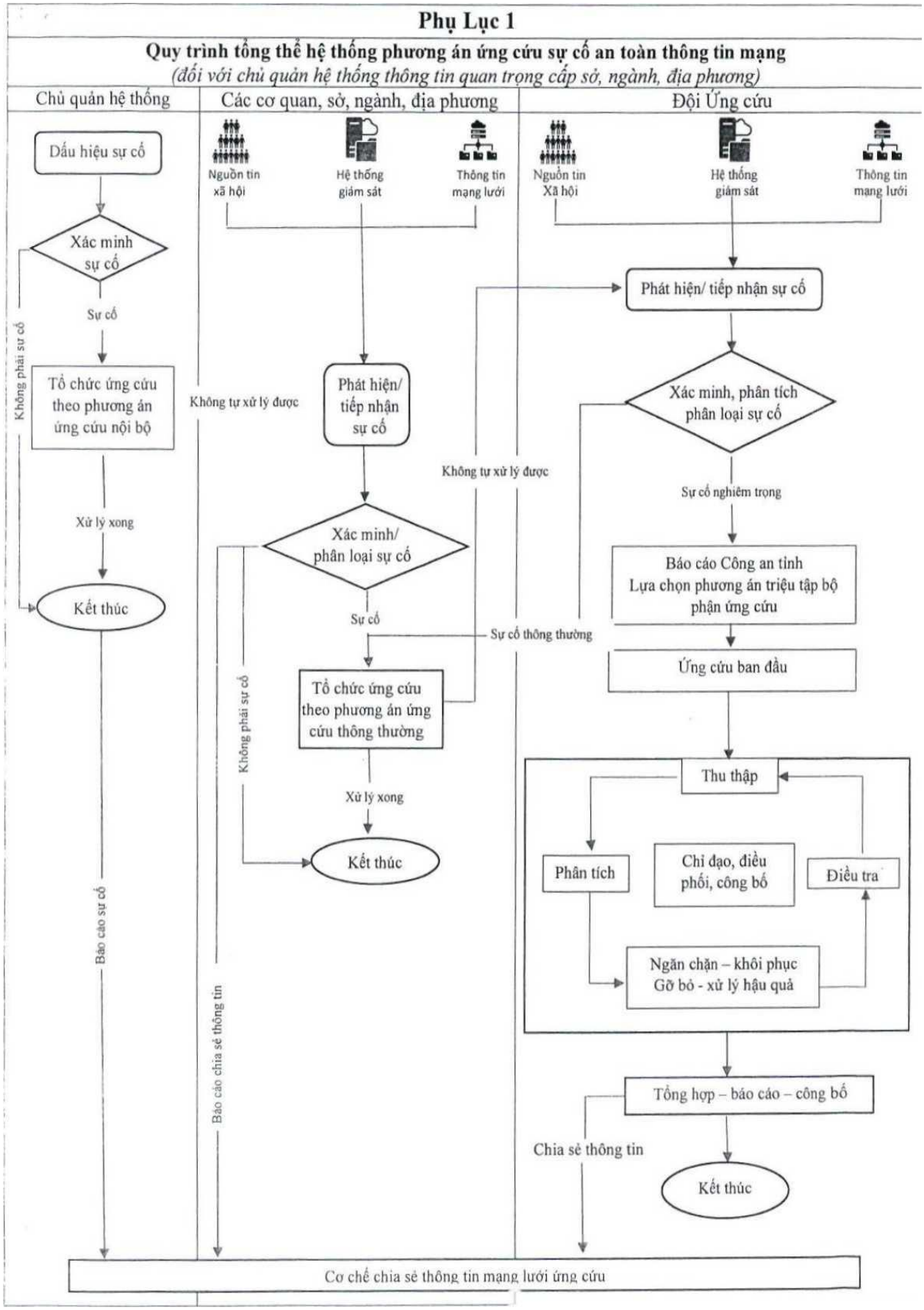
Nơi nhận:
- Bộ Công an
- Thường trực: Tỉnh ủy, HĐND tỉnh (để b/c);
- Chủ tịch UBND tỉnh
- Các Phó Chủ tịch UBND tỉnh
- Cục A05, Bộ Công an (để p/h);
- Ủy ban MTTQ Việt Nam tỉnh;
- Công an tỉnh;
- Các sở, ban, ngành, đơn vị, đoàn thể cấp tỉnh;
- Đảng ủy, UBND các xã, phường;
- Lưu: VT, CNXDKH, TDNC.

TM. UỶ BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Cao Văn Cường

PHỤ LỤC 1

(Ban hành kèm theo Kế hoạch số 150 /KH-UBND ngày 19/ 5 /2026 của UBND tỉnh)



PHỤ LỤC 2

(Ban hành kèm theo Kế hoạch số 150 /KH-UBND ngày 19/ 5 /2026 của UBND tỉnh)

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 (*):……..…

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

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 UCSC □ 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, đóng dấu)

PHỤ LỤC 3

(Ban hành kèm theo Kế hoạch số 150 /KH-UBND ngày 19/ 5 /2026 của UBND tỉnh)

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 (*)[10]:.....
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, dóng dấu)

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