ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 4201 /KH-UBND	*Khánh Hòa, ngày 20 tháng 3 năm 2026*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2026

Thực hiện Nghị quyết số 48-NQ/TU ngày 20/02/2025 của Ban Chấp hành Đảng bộ tỉnh Khánh Hòa thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia và Chương trình công tác năm 2026 của Tiểu ban An ninh mạng tỉnh Khánh Hòa;

Theo đề xuất của Công an tỉnh tại Tờ trình số 3095/TTr-CAT(ANM) ngày 17/3/2026; Ủy ban nhân dân tỉnh ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2026 như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Bảo đảm an toàn hệ thống thông tin đối với các hệ thống thông tin trọng yếu trên địa bàn tỉnh; tăng cường khả năng thích ứng chủ động, linh hoạt trước các nguy cơ, thách thức mất an toàn thông tin mạng; đồng thời thực hiện quyết liệt, hiệu quả các giải pháp ứng phó, khắc phục nhằm duy trì tính liên tục của hệ thống khi xảy ra sự cố mất an toàn thông tin mạng.

- Tập trung nâng cao năng lực giám sát, phát hiện và ứng cứu sự cố an toàn thông tin mạng; đảm bảo khả năng phát hiện sớm và cảnh báo chính xác các sự cố, dấu hiệu tấn công mạng đối với các hệ thống thông tin quan trọng, ứng dụng dịch vụ công nghệ thông tin phục vụ chính quyền điện tử của tỉnh.

- Nâng cao nhận thức và năng lực tự bảo vệ của cán bộ, công chức, viên chức; hình thành đội ngũ người dùng cuối có kỹ năng nhận diện và xử lý tình huống an toàn thông tin cơ bản, nhằm giảm thiểu rủi ro và bảo vệ vững chắc các hệ thống thông tin trọng yếu của tỉnh.

- Đảm bảo nguồn lực và các điều kiện cần thiết để chủ động, kịp thời ứng phó, xử lý hiệu quả các tình huống khẩn cấp về an toàn thông tin; hạn chế thấp nhất các tác động tiêu cực đến hệ thống chính quyền điện tử của tỉnh.

2. Yêu cầu

- Công tác ứng phó sự cố phải dựa trên kết quả khảo sát, đánh giá định kỳ về lỗ hổng và nguy cơ mất an toàn thông tin; từ đó xây dựng các phương án đối phó, kịch bản ứng cứu chi tiết, đảm bảo tính kịp thời và phù hợp với đặc thù hệ thống của từng cơ quan, đơn vị.

- Các phương án ứng cứu sự cố an toàn thông tin mạng phải đặt ra các tiêu chí

nhằm xác định nhanh chóng, chính xác tính chất và mức độ nghiêm trọng của sự cố ngay khi phát sinh; đảm bảo việc ra quyết định xử lý đúng thẩm quyền và ưu tiên nguồn lực phù hợp.

- Xác định cụ thể, chi tiết các nguồn lực về con người, giải pháp công nghệ và dự toán kinh phí triển khai các nội dung trong Kế hoạch, đảm bảo tính khả thi, tiết kiệm và đạt hiệu quả.

- Duy trì cơ chế trao đổi thông tin, chia sẻ kinh nghiệm bảo mật giữa các cơ quan nhà nước trên địa bàn tỉnh; chủ động phối hợp, tranh thủ sự hỗ trợ nghiệp vụ từ các đơn vị chuyên trách của Bộ Công an và các bộ, ngành để xử lý các tình huống phức tạp.

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 ninh mạng, an ninh dữ liệu

- Nội dung thực hiện: Tổ chức tuyên truyền, phổ biến, hướng dẫn nội dung của Luật Bảo vệ bí mật nhà nước, Luật An ninh mạng, Luật Bảo vệ dữ liệu cá nhân và các văn bản hướng dẫn luật, các quy định về công tác ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng.

- Đơn vị chủ trì: Công an tỉnh.

- Đơn vị phối hợp: Sở Khoa học và Công nghệ, các sở, ban, ngành, UBND xã/phường/đặc khu, các cơ quan khối Đảng 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 phó sự cố; tổ chức diễn tập an toàn thông tin

- Nội dung thực hiện: Tổ chức huấn luyện, diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; đào tạo nâng cao kỹ năng, 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: Sở Khoa học và Công nghệ; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa (sau đây viết tắt là Đội UCKCSC); Đơn vị vận hành hệ thống thông tin; Các đơn vị nghiệp vụ của Bộ Công an.

- Thời gian thực hiện: Trong năm 2026.

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

- Nội dung thực hiện:

+ Công an tỉnh xây dựng hoàn thiện hệ thống Trung tâm Giám sát An ninh mạng tỉnh (Trung tâm SOC) giai đoạn 1, thực hiện kết nối liên thông với Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (Trung tâm VNCERT) và mở

rộng phạm vi giám sát đến các cơ quan chuyên môn cấp tỉnh, địa phương; Sở Khoa học và Công nghệ nâng cấp, vận hành hiệu quả Hệ thống Giám sát an ninh mạng tại Trung tâm dữ liệu (Hệ thống SOC). Chủ động giám sát, rà quét và bóc gỡ mã độc; tập trung phân tích, xác minh và cảnh báo sớm các nguy cơ, lỗ hổng bảo mật nhằm phòng ngừa sự cố và quản trị rủi ro hệ thống. Chuẩn hóa quy trình, định mức kỹ thuật về an toàn thông tin; đẩy mạnh công tác tuyên truyền, tập huấn nâng cao nhận thức và kỹ năng ứng phó sự cố cho cán bộ, công chức, viên chức.

+ Rà soát, đánh giá thực trạng công tác bảo mật, xác định các lĩnh vực trọng điểm có nguy cơ cao để tập trung triển khai các biện pháp bảo vệ, phòng ngừa; đẩy mạnh nâng cấp giao thức bảo mật cho các cổng thông tin điện tử và hạ tầng mạng của cơ quan nhà nước. Ưu tiên bố trí cán bộ có năng lực chuyên môn và phẩm chất tốt để đảm nhiệm những vị trí quan trọng trong quản lý, vận hành các hệ thống thông tin thuộc phạm vi quản lý; đảm bảo lực lượng đủ khả năng xử lý các tình huống phát sinh tại chỗ.

- Đơn vị chủ trì: Công an tỉnh, Sở Khoa học và Công nghệ; Đội UCKCSC; Đơn vị vận hành hệ thống thông tin.

- 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 đối phó, ứng cứu, khắc phục sự cố

- Nội dung thực hiện: Trang bị, nâng cấp trang thiết bị chuyên dụng và gia hạn bản quyền phần mềm bảo mật. Duy trì hoạt động hiệu quả của Đội ứng cứu sự cố tỉnh; kết hợp thuê dịch vụ kỹ thuật chuyên sâu và xây dựng mạng lưới chuyên gia tư vấn để xử lý các tình huống phức tạp. Kết nối, tham gia các hoạt động của Mạng lưới ứng cứu sự cố quốc gia; chủ động xây dựng và vận hành các phương án nhân lực, thiết bị và dự phòng nguồn lực tài chính, kỹ thuật để sẵn sàng ứng phó linh hoạt theo từng cấp độ sự cố, đảm bảo tính khả thi và hiệu quả.

- Đơn vị chủ trì: Công an tỉnh; Sở Khoa học và Công nghệ; Đội UCKCSC; Đơn vị vận hành hệ thống thông tin.

- 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 các hệ thống thông tin; đánh giá, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra với các hệ thống thông tin; 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 đối 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 chủ trì: Đơn vị vận hành hệ thống thông tin.

- 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: Đơn vị vận hành 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)*.

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

- Nội dung thực hiện:

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

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

- Đơn vị chủ trì: Đơn vị vận hành hệ thống thông tin.

- 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

2.1 Trình tự thực hiện tại Phụ lục 1 đính kèm.

- Quy trình 01: Ứng cứu sự cố an toàn thông tin mạng nghiêm trọng

Áp dụng: Các sự cố an toàn thông tin mạng nghiêm trọng mà đơn vị vận hành HTTT, các sở, ban ngành, địa phương, cơ quan khối Đảng và Đội UCKCSC của tỉnh không đủ khả năng tự kiểm soát, xử lý được sự cố.

- Quy trình 02: Ứng cứu sự cố an toàn thông tin mạng thông thường

Áp dụng: Các sự cố an toàn thông tin mạng còn lại và không thuộc trường hợp áp dụng Quy trình 01.

2.2. Báo cáo sự cố an toàn thông tin mạng

a) Đơn vị vận hành hệ thống thông tin, các sở, ban, ngành, địa phương, cơ quan khối Đảng có trách nhiệm báo cáo sự cố tới Đội UCKCSC. Báo cáo sự cố phải được thực hiện ngay 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); nội dung báo cáo tại điểm c 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, các sở, ban ngành, địa phương, cơ quan khối Đảng báo cáo Đội UCKCSC.

- Đội UCKCSC trao đổi với đơn vị vận hành hệ thống thông tin, các sở, ban, ngành, địa phương, cơ quan khối Đảng; 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, Đội UCKCSC.

2.3. Tiếp nhận, phát hiện, phân loại và xử lý ban đầu 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 vận hành hệ thống thông tin, các sở, ban ngành, địa phương, cơ quan khối Đảng, 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, các sở, ban ngành, địa phương, cơ quan khối Đảng 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.

b) Đơn vị vận hành hệ thống thông tin, các sở, ban ngành, địa phương, cơ quan khối Đảng 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 Công an tỉnh, Đội UCKCSC.

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

a) Đơn vị vận hành hệ thống thông tin, các sở, ban ngành, địa phương, cơ quan khối Đảng 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 vận hành hệ thống thông tin, các sở, ban ngành, địa phương, cơ quan khối Đảng 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 quản lý hệ thống hoặc gây ảnh hưởng xấu tới xã hội.

- Đơn vị vận hành hệ thống thông tin, các sở, ban ngành, địa phương, cơ quan khối Đảng phải phối hợp chặt chẽ, cung cấp đầy đủ thông tin để Đội UCKCSC 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: Đơn vị vận hành hệ thống thông tin, các sở, ban ngành, địa phương, cơ quan khối Đảng 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 Đội UCKCSC, Công an tỉnh.

- Ngăn chặn, xử lý các hành vi đã được phát hiện: Đội UCKCSC, 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 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: Các sở, ban ngành, địa phương, cơ quan khối Đảng có trách nhiệm triển khai xử lý 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.

g) Xác minh nguyên nhân và truy tìm nguồn gốc: Đội UCKCSC, 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 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; (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; (6) Dự đoán khả năng xảy ra các tấn công tương tự và thiệt hại.

h) 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.

m) Tổng kết: Đội UCKCSC, Công an tỉnh phối hợp với đơn vị vận hành hệ thống thông tin, các sở, ban ngành, địa phương, cơ quan khối Đảng, 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 *(thực hiện việc lưu hồ sơ, tài liệu lưu trữ; xây dựng, đúc rút các bài học, kinh nghiệm; đề xuất các kiến nghị về kỹ thuật, chính sách để hạn chế thiệt hại khi xảy ra sự cố tương tự; báo cáo cơ quan cấp trên, tổ chức họp báo hoặc gửi thông tin cho truyền thông nếu cần thiết)* để kết thúc hoạt động ứng cứu sự cố khẩn cấp. 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*).

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

a) Đối với mỗi hệ thống thông tin, chương trình ứng dụng, đơn vị vận hành hệ thống thông tin, các sở, ban ngành, địa phương, cơ quan khối Đảng cần xây dựng

tình huống, kịch bản sự cố cụ thể và đưa ra phương án đối phó, ứng cứu sự cố tương ứng. Việc xây dựng phương án đối 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 đối 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 đối 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, sử dụng 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 đối 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, đối 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 được bố trí trong dự toán chi ngân sách nhà nước hằng năm của các cơ quan, đơn vị, địa phương theo phân cấp ngân sách hiện hành, phù hợp với khả năng cân đối ngân sách và theo quy định của Luật Ngân sách nhà nước và các văn bản hướng dẫn có liên quan.

Các sở, ban ngành, đơn vị, địa phương căn cứ nhiệm vụ được giao tại Kế hoạch chủ động xây dựng dự toán kinh phí thực hiện hằng năm, gửi cơ quan tài chính cùng cấp tổng hợp, trình cấp có thẩm quyền xem xét, quyết định theo quy định.

IV. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành; UBND các xã/phường/đặc khu; các cơ quan khối Đảng

- Thủ trưởng các sở, ban ngành; Giám đốc Công an tỉnh; Chủ tịch UBND các xã/phường/đặc khu 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 2026 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.

- Việc quản lý, sử dụng và thanh quyết toán kinh phí thực hiện Kế hoạch phải bảo đảm đúng mục đích, tiết kiệm, hiệu quả và tuân thủ các quy định của pháp luật về ngân sách nhà nước, đầu tư công, quản lý tài sản công và các quy định có liên quan. Trường hợp phát sinh nhiệm vụ cần bố trí kinh phí ngoài dự toán được giao, các cơ quan, đơn vị báo cáo cấp có thẩm quyền xem xét, quyết định theo quy định.

- Rà soát, kiện toàn các quyết định (nếu có thay đổi): Phân công lãnh đạo phụ trách an toàn thông tin; thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về an toàn thông tin mạng của cơ quan, đơn vị; phân công cán bộ, công chức

chuyên trách về an toàn thông tin mạng tại cơ quan, đơn vị, địa phương; kịp thời gửi thông báo về Công an tỉnh khi có thay đổi nhân sự 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, Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) và hướng dẫn của Công an tỉnh – Cơ quan Thường trực Tiểu ban An ninh mạng.

- Thực hiện xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống 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, nay là Bộ Khoa học và Công nghệ) 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 đầy đủ 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. Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh

- Chủ trì, điều phối hoạt động ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh và các nhiệm vụ được giao tại Kế hoạch này; tổng hợp kết quả, báo cáo Công an tỉnh - Cơ quan Thường trực Tiểu ban An ninh mạng theo quy định.

- Thực hiện các nhiệm vụ khác được giao tại Điều 2 Quyết định số 2162/QĐ-UBND ngày 19/11/2025 của UBND tỉnh về việc kiện toàn Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.

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

- Chủ trì, phối hợp, theo dõi, đôn đốc các sở, ban, ngành, địa phương tổ chức thực hiện Kế hoạch; tổng hợp, báo cáo UBND tỉnh kết quả thực hiện theo quy định.

- 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.

4. Sở Khoa học và Công nghệ

Phối hợp chặt chẽ với Công an tỉnh, Đội UCKCSC thực hiện các nội dung của Kế hoạch này; nghiên cứu, cập nhật giải pháp quản trị, vận hành hệ thống thông tin quan trọng. Hướng dẫn các cơ quan, đơn vị khai thác hệ thống dùng chung an toàn,

hiệu quả; kịp thời rà soát, ban hành hoặc sửa đổi các quy chế, quy trình vận hành. Chủ động phối hợp với Công an tỉnh phòng ngừa, ngăn chặn tấn công mạng và xử lý khắc phục các điểm yếu, lỗ hổng bảo mật hệ thống, bảo đảm an toàn thông tin phải song hành với quá trình chuyển đổi số.

5. 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, địa phương kịp thời phối hợp với Công an tỉnh để tổng hợp, báo cáo UBND tỉnh xem xét, giải quyết theo thẩm quyền./.

Nơi nhận:
- Cục A05 - Bộ Công an (b/cáo);
- Thường trực Tỉnh ủy (b/cáo);
- Thường trực HĐND tỉnh (b/cáo);
- Chủ tịch và các PCT UBND tỉnh;
- Thường trực UBMTTQVN tỉnh;
- Tiểu ban ANM tỉnh;
- Các sở, ban ngành;
- Cơ quan khối Đảng;
- UBND các xã, phường, đặc khu;
- Các đoàn thể chính trị - xã hội;
- Doanh nghiệp nhà nước;
- Doanh nghiệp viễn thông;
- VPUB: LĐ, các phòng, ban, trung tâm;
- Lưu: VT. NNN

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

ỦY BAN NHÂN DÂN TỈNH KHÁNH HÒA

Nguyễn Thanh Hà