UBND TỈNH KHÁNH HÒA **SỞ NỘI VỤ** Số: 1319/KH-SNV	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc** *Khánh Hòa, ngày 09 tháng 02 năm 2026*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng tại Sở Nội vụ năm 2026

Thực hiện Kế hoạch số 5479/KH-UBND ngày 08/05/2025 của UBND tỉnh Khánh Hòa về ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2026, Sở Nội vụ xây dựng Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng tại Sở Nội vụ năm 2026, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Đảm bảo an toàn thông tin mạng của Sở Nội vụ, khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ đe dọa mất an toàn thông tin mạng; đề ra các giải pháp ứng phó kịp thời khi gặp sự cố mất an toàn thông tin mạng.

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

- Đảm bảo các nguồn lực, điều kiện cần thiết để sẵn sàng triển khai kịp thời, hiệu quả phương án ứng cứu sự cố bảo đảm an toàn thông tin mạng.

2. Yêu cầu

- Triển khai công tác ứng phó sự cố, bảo đảm an toàn thông tin mạng tại Sở Nội vụ phải bám sát kết quả rà soát, đánh giá nguy cơ đối với các hệ thống thông tin, cơ sở dữ liệu phục vụ công tác quản lý nhà nước về Nội vụ; bảo đảm phối hợp kịp thời với cơ quan chuyên trách an toàn thông tin và các đơn vị liên quan khi xảy ra sự cố.

- Phương án đối phó, ứng cứu sự cố an toàn thông tin mạng phải đặt ra được 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 đảm bảo, giải pháp tổ chức thực hiện để triển khai các nội dung của Kế hoạch, đảm bảo khả thi, hiệu quả.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác đảm bảo an toàn thông tin giữa các cơ quan nhà nước trên địa bàn tỉnh; tăng cường sự phối hợp, hỗ trợ của cơ quan điều phối quốc gia về ứng cứu sự cố *(Trung tâm*

Ứng cứu khẩn cấp không gian mạng Việt Nam, 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 phổ biến đến toàn thể công chức, viên chức, tuyên truyền trên Trang Thông tin điện tử của Sở các văn bản về an toàn thông tin: Luật An toàn thông tin mạng ngày 19/11/2015, Luật An ninh mạng ngày ngày 10/12/2025; Quyết định số 05/2017/QĐ-TTg ngày 16/03/2017 của Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; Quyết định số 11/2026/QĐ-UBND ngày 31/01/2026 của Ủy ban nhân dân tỉnh ban hành Quy chế bảo đảm an ninh mạng, an toàn thông tin trên địa bàn tỉnh Khánh Hòa; Quyết định số 83/QĐ-SNV ngày 29/7/2025 của Sở Nội vụ ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin tại Sở Nội vụ Khánh Hòa.

- Đơn vị thực hiện: Phòng Pháp chế

- Đơn vị phối hợp: Các cơ quan, đơn vị thuộc và trực thuộc Sở.

- Thời gian thực hiện: Thường xuyên trong năm.

b) Tham gia các chương trình đào tạo, bồi dưỡng kỹ năng đánh giá, ứng phó sự cố

- Nội dung thực hiện: tham gia các chương trình 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 Kế hoạch, Thông báo triệu tập của Công an tỉnh.

- Đơn vị thực hiện: Văn phòng Sở.

- Đơn vị phối hợp: Các cơ quan, đơn vị thuộc và trực thuộc Sở.

- 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:

+ 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 mặt trọng tâm, trọng điểm có nguy cơ, từ đó tập trung triển khai các biện pháp bảo vệ, phòng ngừa; chú trọng vấn đề nâng cấp giao thức bảo mật cho các trang thông tin điện tử, cơ sở hạ tầng mạng trong hệ thống thông tin của cơ quan, các đơn vị trực thuộc Sở.

- Đơn vị thực hiện: Văn phòng Sở; các cơ quan, đơn vị thuộc và trực thuộc Sở.

- Đơn vị phối hợp: Các đơn vị có liên quan.

- 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 ứng cứu, 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; tham gia các hoạt động của mạng lưới ứng cứu sự cố.

- Đơn vị thực hiện: Văn phòng Sở; các cơ quan, đơn vị thuộc và trực thuộc Sở.

- Đơn vị phối hợp: Các đơn vị có liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

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

- Nội dung thực hiện: Đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của hệ thống thông tin và các đối tượng cần bảo vệ; 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 đối phó, ứng cứu, khắc phục sự cố của cơ quan, các đơn vị thuộc, trực thuộc Sở *(bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có)*.

- Đơn vị thực hiện: Văn phòng Sở; các cơ quan, đơn vị thuộc và trực thuộc Sở.

- Đơn vị phối hợp: Công an tỉnh, Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; các nhà thầu cung cấp dịch vụ an toàn thông tin mạng (nếu có); các đơn vị khác liên quan.

- Thời gian thực hiện: Văn phòng Sở; các cơ quan, đơn vị thuộc và trực thuộc Sở chủ trì đánh giá, kiểm tra hệ thống thông tin định kỳ 06 tháng *(trước ngày 10/06)*, 01 năm *(trước ngày 05/12)*.

e) 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 để có thể nhanh chóng xác định được tính chất, mức độ nghiêm trọng khi sự cố xảy ra. Các cơ quan, đơn vị thuộc, trực thuộc Sở quản lý, vận hành hệ thống thông tin, chương trình ứng dụng phải xây dựng phương án đối phó, ứng cứu sự cố theo hướng dẫn của Công an tỉnh và các đơn vị nghiệp vụ thuộc Bộ Công an.

- Đơn vị chủ trì: Văn phòng Sở; các cơ quan, đơn vị thuộc và trực thuộc Sở.

- Đơn vị phối hợp: Công an tỉnh; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); các đơn vị khác liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

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 kèm theo Kế hoạch này.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện kế hoạch này được bố trí từ nguồn ngân sách hàng năm của Sở Nội vụ và các nguồn hợp pháp khác.

IV. TỔ CHỨC THỰC HIỆN

1. Các cơ quan, đơn vị thuộc và trực thuộc Sở

- Các cơ quan, đơn vị thuộc và trực thuộc Sở được giao quản lý, vận hành hệ thống thông tin: thực hiện xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Điều 14 và Điều 15 Nghị định số 85/2016/NĐ-CP và theo hướng dẫn tại Thông tư số 12/2022/TT-BTTTT.

- Định kỳ hằng năm, gửi báo cáo tình hình, kết quả về Văn phòng Sở để tổng hợp báo cáo UBND tỉnh hoặc báo cáo đột xuất khi có yêu cầu từ cấp có thẩm quyền.

- Căn cứ vào chức năng, nhiệm vụ được giao, tổ chức thực hiện Kế hoạch Ứng phó sự cố bảo đảm an toàn thông tin mạng phù hợp với điều kiện của đơn vị.

2. Văn phòng Sở

- Làm đầu mối, tổ chức hoạt động ứng cứu sự cố, tổ chức thực hiện việc tiếp nhận và xử lý các sự cố về an toàn hệ thông tin mạng thuộc Sở quản lý; tham gia hoạt động ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng khi có yêu cầu từ Công an tỉnh - Cơ quan thường trực hoặc Cơ quan điều phối.

- Tham gia ý kiến về mặt chuyên môn đối với hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo thẩm quyền quy định tại Khoản 1, Khoản 2 Điều 12 và Khoản 5 Điều 15 Nghị định số 85/2016/NĐ-CP và theo hướng dẫn tại Thông tư số 12/2022/TT-BTTTT và Nghị định số 85/2016/NĐ-CP.

- Hướng dẫn, kiểm tra, báo cáo việc thực hiện Kế hoạch ứng phó sự cố bảo đảm an toàn thông tin mạng của Sở theo quy định.

Đề nghị các cơ quan, đơn vị triển khai thực hiện ./.

Nơi nhận: *(VBĐT)*
- UBND tỉnh *(báo cáo)*;
- Công an tỉnh;
- Các cơ quan, đơn vị thuộc Sở;
- Lãnh đạo Sở;
- Lưu: VT, VP.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ NỘI VỤ
TỈNH KHÁNH HÒA

Huỳnh Mạnh Thắng

PHỤ LỤC
QUY TRÌNH ỨNG CỨU SỰ CỐ AN TOÀN THÔNG TIN MẠNG
(Kèm theo Kế hoạch số 1319 /KH-SNV ngày 09 /02/2026 của Sở Nội vụ tỉnh Khánh Hòa)

STT	QUY TRÌNH	NỘI DUNG THỰC HIỆN	ĐƠN VỊ CHỦ TRÌ	ĐƠN VỊ PHỐI HỢP
I	**TIẾP NHẬN, PHÂN TÍCH, ỨNG CỨU BAN ĐẦU VÀ THÔNG BÁO SỰ CỐ**			
1	Tiếp nhận, xác minh sự cố	Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể từ các nguồn bên trong và bên ngoài. Khi phân tích, xác minh sự cố đã xảy ra, cần tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố	Văn phòng Sở; các cơ quan, đơn vị thuộc và trực thuộc Sở	Công an tỉnh; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa
2	Triển khai các bước ưu tiên ứng cứu ban đầu	Căn cứ vào bản chất, dấu hiệu của sự cố tổ chức triển khai các bước ưu tiên ban đầu để xử lý sự cố theo kế hoạch ứng phó sự cố đã được cấp thẩm quyền phê duyệt hoặc theo hướng dẫn của Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng tỉnh Khánh Hòa	Văn phòng Sở; các cơ quan, đơn vị thuộc và trực thuộc Sở	Công an tỉnh; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa
3	Triển khai lựa chọn phương án ứng cứu	Căn cứ theo Kế hoạch Ứng phó sự cố của UBND tỉnh, Sở Nội vụ ban hành hoặc theo hướng dẫn của Cơ quan trường trực ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh để lựa chọn phương án ngăn chặn và xử lý sự cố; báo cáo, đề xuất Sở Nội vụ hoặc Ban Chỉ đạo Chuyển đổi số tỉnh Khánh Hòa để xin ý kiến chỉ đạo (nếu cần thiết)	Văn phòng Sở; các cơ quan, đơn vị thuộc và trực thuộc Sở	Công an tỉnh; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa
4	Chỉ đạo xử lý sự cố *(trong trường hợp sự cố nghiêm trọng, cần triệu tập Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Khánh Hòa và đề nghị Cơ quan điều phối quốc gia hỗ trợ)*	Căn cứ theo báo cáo, đề xuất của Sở Nội vụ. Ban chỉ đạo Chuyển đổi số phối hợp chủ quản hệ thống thông tin và tham khảo ý kiến Cơ quan điều phối (nếu cần) thực hiện chỉ đạo Cơ quan chuyên trách Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa triển khai công tác ứng cứu, xử lý	Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và Đề án 06 tỉnh Khánh Hòa	Văn phòng Sở, các đơn vị thuộc và trực thuộc Sở
5	Báo cáo sự cố	Sau khi đã triển khai các bước ưu tiên ứng cứu ban đầu, đơn vị quản lý vận hành hệ thống thông tin thông báo, báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan theo quy định tại Điều 9 Thông tư số 20/2017/TT-	Văn phòng Sở; các cơ quan, đơn vị thuộc và trực Sở	Công an tỉnh; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.

STT	QUY TRÌNH	NỘI DUNG THỰC HIỆN	ĐƠN VỊ CHỦ TRÌ	ĐƠN VỊ PHỐI HỢP
		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		
6	Điều phối công tác ứng cứu	Căn cứ vào tính chất sự cố, đề nghị hỗ trợ của Đơn vị quản lý, vận hành hệ thống thông tin, Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa, Cơ quan điều phối quốc gia hoặc Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh thực hiện công tác điều phối, giám sát cơ chế phối hợp, chia sẻ thông tin theo phạm vi, chức năng, nhiệm vụ của mình để huy động nguồn lực ứng cứu sự cố	Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và Đề án 06 tỉnh Khánh Hòa; Cơ quan điều phối quốc gia (Trung tâm ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); Công an tỉnh	Văn phòng Sở, các đơn vị trực thuộc và trực thuộc Sở
II	**TRIỂN KHAI ỨNG CỨU, NGĂN CHẶN VÀ XỬ LÝ SỰ CỐ**			
1	Triển khai ứng cứu, ngăn chặn và xử lý sự cố	Triển khai thu thập chứng cứ, phân tích, xác định phạm vi, đối tượng bị ảnh hưởng; phân tích, xác định nguồn gốc tấn công, tổ chức ứng cứu và ngăn chặn, giảm thiểu tác động, thiệt hại đến hệ thống thông tin	Văn phòng Sở, các cơ quan, đơn vị thuộc Sở	Công an tỉnh
III	**XỬ LÝ SỰ CỐ, GỠ BỎ, KHÔI PHỤC VÀ XỬ LÝ VI PHẠM**			
1	Xử lý, gỡ bỏ sự cố	Sau khi đã triển khai ngăn chặn sự cố, Văn phòng Sở, các cơ quan, đơn vị thuộc Sở chịu trách nhiệm khẩn trương ngăn chặn sự cố, đồng thời tiêu diệt, gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của hệ thống thông tin (phối hợp với Công an tỉnh và Đội Ứng khẩn cấp sự cố an toàn thông tin mạng tỉnh nếu cần thiết)	Văn phòng Sở, các cơ quan, đơn vị thuộc Sở	Công an tỉnh; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa
2	Khôi phục	Đơn vị quản lý, vận hành hệ thống thông tin chủ trì phối hợp với các đơn vị liên quan triển khai các hoạt động khôi phục hệ thống thông tin, dữ liệu và kết nối; cấu hình hệ thống an toàn; bổ sung các thiết bị, phần cứng, phần mềm bảo đảm an toàn thông tin của hệ thống thông tin	Văn phòng Sở, các cơ quan, đơn vị thuộc Sở	Công an tỉnh; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa)

STT	QUY TRÌNH	NỘI DUNG THỰC HIỆN	ĐƠN VỊ CHỦ TRÌ	ĐƠN VỊ PHỐI HỢP
3	Kiểm tra, đánh giá an toàn hệ thống thông tin sau khi khôi phục	Đơn vị quản lý, vận hành hệ thống thông tin và các đơn vị liên quan triển khai kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống thông tin chưa bảo đảm an toàn, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân và tổ chức ứng cứu các bước tương ứng tại Khoản 2.2 và Khoản 2.3 của Kế hoạch này để xử lý dứt điểm, khôi phục hoạt động của hệ thống thông tin trở lại bình thường	Văn phòng Sở, các cơ quan, đơn vị thuộc Sở	Công an tỉnh; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa
4	Xử lý vi phạm	Đơn vị quản lý, vận hành hệ thống thông tin phối hợp với các đơn vị liên quan làm rõ nguyên nhân, phân tích ngăn chặn, xử lý kịp thời các đối tượng tấn công, phá hoại, hạn chế đến mức thấp nhất hậu quả xảy ra; nếu nguyên nhân do thiếu trách nhiệm, vi phạm quy định về an toàn thông tin, tùy theo mức độ vi phạm mà tổ chức kiểm điểm rút kinh nghiệm hoặc xử lý theo quy định của pháp luật; nếu nguyên nhân do tác động của các đối tượng tấn công bên ngoài cần thu thập, xác minh, tổng hợp báo cáo chủ quản hệ thống thông tin và cơ quan có thẩm quyền xem xét, điều tra xử lý	Văn phòng Sở, các cơ quan, đơn vị thuộc Sở	Công an tỉnh; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa và các cơ quan có thẩm quyền
IV	**TỔNG KẾT, ĐÁNH GIÁ**			
1	Tổng kết và đánh giá	Đơn vị quản lý, vận hành hệ thống thông tin bị sự cố phối hợp với Cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh và Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa triển khai tổng hợp toàn bộ các thông tin, báo cáo, phân tích có liên quan đến sự cố, công tác triển khai phương án ứng cứu sự cố, báo cáo Sở Nội vụ, Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa; tổ chức phân tích nguyên nhân, rút kinh nghiệm trong hoạt động xử lý sự cố và đề xuất các biện pháp bổ sung nhằm phòng ngừa, ứng cứu đối với các sự cố tương tự trong tương lai	Văn phòng Sở, các cơ quan, đơn vị thuộc Sở	Công an tỉnh, Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa