ỦY BAN NHÂN DÂN **TỈNH KHÁNH HÒA**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 2517 /KH-UBND	*Khánh Hòa, ngày 17 tháng 3 năm 2023*

KẾ HOẠCH
Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Khánh Hòa năm 2023

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 và triển khai Kế hoạch số 13784/KH-UBND ngày 31/12/2020 của UBND tỉnh Khánh Hòa 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; 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 2023, 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 trên mạng; đề ra các giải pháp ứng phó khi gặp 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, dịch vụ công nghệ thông tin phục vụ chính phủ điện tử của tỉnh.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an toàn thông tin đối với lực lượng công chức, viên chức.

- 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.

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 của các cơ quan nhà nước trên địa bàn tỉnh để đưa ra phương án đối phó, ứng cứu sự cố tương ứng, kịp thời, phù hợp.

- Phương án đối 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 Thông tin và Truyền thông.

II. NHIỆM VỤ TRIỂN KHAI

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

1.1. 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, 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; 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; 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; 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 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; Kế hoạch số 13784/KH-UBND ngày 31/12/2020 của UBND tỉnh Khánh Hòa 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 và các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn về an toàn thông tin mạng trên các phương tiện thông tin đại chúng, Cổng Thông tin điện tử của tỉnh, Trang thông tin điện tử của sở, ban, ngành, UBND các huyện, thị xã, thành phố.

- Đơn vị thực hiện: Sở Thông tin và Truyền thông.

- Đơn vị phối hợp: Các sở, ban, ngành, Công an tỉnh, UBND các huyện, thị

xã, thành phố và các đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên trong năm.

1.2. Triển khai các chương trình đào tạo, bồi dưỡng kỹ năng đánh giá, ứng phó sự cố

- 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 Bộ Thông tin và Truyền thông.

- Đơn vị thực hiện: Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.

- Đơn vị phối hợp: Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, UBND các huyện, thị xã, thành phố; Công an tỉnh); Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); các đơn vị liên quan.

- Thời gian thực hiện: Dự kiến tháng 6/2023.

1.3. 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 UBND cấp huyện; 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 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: Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành, UBND các huyện, thị xã, thành phố; Công an tỉnh).

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); Trung tâm Giám sát an toàn không gian mạng quốc gia; các đơn vị liên quan khác.

- Thời gian thực hiện: Thường xuyên trong năm.

1.4. 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, 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 đối phó, ứng cứu, khắc phục khi sự cố xảy ra; tổ chức hoạt động của đội ứng cứu sự cố; 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.

- Đơn vị thực hiện: Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành; UBND các huyện, thị xã, thành phố; Công an tỉnh).

- Đơn vị phối hợp: Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); các đơn vị liên quan khác.

- Thời gian thực hiện: Thường xuyên trong năm.

1.5. 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 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 thực hiện: Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành; UBND các huyện, thị xã, thành phố; Công an tỉnh).

- Đơn vị phối hợp: Sở Thông tin và Truyền thông; 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: Cơ quan chủ quản hệ thống thông tin tự chủ trì đánh giá, kiểm tra hệ thống thông tin định kỳ 06 tháng/01 lần.

1.6. 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 và chương trình ứng dụng, 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 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. Các cơ quan 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 Sở Thông tin và Truyền thông và các đơn vị chuyên môn thuộc Bộ Thông tin và Truyền thông.

- Đơn vị thực hiện: Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành; UBND các huyện, thị xã, thành phố; Công an tỉnh).

- Đơn vị phối hợp: Sở Thông tin và Truyền thông; 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: 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 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 tỉnh.

IV. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành; UBND các huyện, thị xã, thành phố; Công an tỉnh

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

- Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch chuyển đổi số và bảo đảm an toàn thông tin mạng hàng năm của cơ quan, đơn vị để triển khai các nhiệm vụ được giao tại Kế hoạch này hoặc chủ động xây dựng dự toán kinh phí chi tiết, gửi về Sở Thông tin và Truyền thông tổng hợp để gửi Sở Tài chính thẩm định, trình UBND tỉnh phê duyệt, cấp kinh phí thực hiện các nhiệm vụ.

- 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, địa phương mình; kịp thời thông báo về Sở Thông tin và Truyền thông khi có sự thay đổi cán bộ, công chức chuyên trách về an toàn thông tin mạng tại cơ quan, địa phương hoặc cán bộ, công chức, viên chức đang là thành viên tham gia

Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa.

- 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 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.

- Khẩn trương 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, gửi về Sở Thông tin và Truyền thông thẩm định.

- Cử cán bộ tham gia các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn 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. Sở Thông tin và Truyền thông

- 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, UBND các huyện, thị xã, thành phố trong việc triển khai thực hiện Kế hoạch này; định kỳ hàng quý, 06 tháng, cả năm báo cáo kết quả thực hiện cho UBND tỉnh để theo dõi và chỉ đạo.

- Sở Thông tin và Truyền thông là thành viên Mạng lưới ứng cứu sự cố an toàn thông tin mạng quốc gia, thực hiện trách nhiệm, quyền hạn theo quy định tại Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc.

- Thẩm định, phê duyệt hoặc cho 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; tham mưu trình UBND tỉnh xem xét, phê duyệt Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin đối với các hệ thống thông tin thuộc thẩm quyền phê duyệt của UBND tỉnh.

- Xây dựng nội dung, lập dự toán kinh phí lồng ghép trong Kế hoạch chuyển đổi số của tỉnh để bảo đảm cho hoạt động của Đơn vị chuyên trách ứng cứu sự cố (Sở Thông tin và Truyền thông) và Đội Ứng cứu khẩn cấp sự cố an toàn thông tin

mạng tỉnh.

3. 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 Sở Thông tin và Truyền thông chủ trì lập, Sở Tài chính tổng hợp, cân đối theo khả năng ngân sách để tham mưu trình cấp thẩm quyền bố trí kinh phí từ nguồn vốn sự nghiệp 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 Sở Thông tin và Truyền thông để tổng hợp, báo cáo UBND tỉnh xem xét, giải quyết theo thẩm quyền./.

Nơi nhận:
- Bộ TTTT (VBĐT - để b/c);
- TT. Tỉnh ủy (để b/c);
- TT. HĐND tỉnh (để b/c);
- Chủ tịch và các PCT/UBND tỉnh (để b/c);
- TT. UBMTTQVN tỉnh;
- Các sở, ban, ngành;
- Công an tỉnh;
- UBND các huyện, TX, TP;
- Các đoàn thể chính trị - xã hội;
- Các đơn vị sự nghiệp;
- Lãnh đạo VPUBND tỉnh;
- Phòng HC-TC;
- Lưu: VT,TNT, LH, ĐL.

KT.CHỦ TỊCH
PHÓ CHỦ TỊCH

Đinh Văn Thiệu

PHỤ LỤC

QUY TRÌNH ỨNG CỨU, XỬ LÝ KHẨN CẤP SỰ CỐ TẤN CÔNG MẠNG

(Ban hành kèm theo Kế hoạch số 2517/KH-UBND ngày 17 tháng 3 năm 2023 của UBND 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	Đơn vị quản lý, vận hành hệ thống thông tin.	Sở Thông tin và Truyền thông; 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)
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 trên địa bàn tỉnh hoặc Cơ quan điều phối quốc gia	Đơn vị quản lý, vận hành hệ thống thông tin.	Sở Thông tin và Truyền thông; 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)
3	Triển khai lựa chọn phương án ứng cứu	Căn cứ theo Kế hoạch Ứng phó sự cố do UBND tỉnh 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 Chủ quản hệ thống thông tin hoặc Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa để xin ý kiến chỉ đạo (nếu cần thiết)	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; 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)
4	Chỉ đạo xử lý sự cố *(trong trường hợp sự cố nghiêm trọng, cần triệu tập*	Căn cứ theo báo cáo, đề xuất của Đơn vị quản lý, vận hành hệ thống thông tin, 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)	Ban chỉ đạo chuyển đổi số tỉnh Khánh Hòa	Chủ quản hệ thống thông tin

	Đội Ứng cứu sự cố an toàn thông tin mạng tỉnh Khánh Hòa và đề nghị Cơ quan điều phối quốc gia hỗ trợ)	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		
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 tổ chức 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-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 và quy định nội bộ (nếu có)	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; 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)
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 chuyển đổi số tỉnh Khánh Hòa; Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); Sở Thông tin và Truyền thông	Đơn vị quản lý, vận hành hệ thống thông tin (các sở, ban, ngành; UBND các huyện, thị xã, thành phố); Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa
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	Đơn vị quản lý, vận hành hệ thống thông tin; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng	Sở Thông tin và Truyền thông; Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC)

			tỉnh Khánh Hòa	
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, đơn vị quản lý, vận hành hệ thống thông tin 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 Sở Thông tin và Truyền thông và Đội Ứng khẩn cấp sự cố an toàn thông tin mạng tỉnh nếu cần thiết)	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; 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)
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 thôn tin	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; 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)
3	Kiểm tra, đánh giá an toàn hệ thống thông tin sau khai 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	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; 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)
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	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông; Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa; Cục phòng chống tội phạm sử dụng công nghệ cao (Bộ Công an); Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt

		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 (thuộc Bộ Thông tin và Truyền thông, Cục phòng chống tội phạm sử dụng công nghệ cao) xem xét, điều tra xử lý		Nam - VNCERT/CC)
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 Chủ quản hệ thống thông tin, Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa và Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC); 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	Đơn vị quản lý, vận hành hệ thống thông tin	Sở Thông tin và Truyền thông, Đội Ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Khánh Hòa, Ban Chỉ đạo chuyển đổi số tỉnh Khánh Hòa, Cơ quan điều phối quốc gia (Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam - VNCERT/CC)