

Số: /KH-UBND

Đồng Tháp, ngày tháng năm 2021

KẾ HOẠCH

Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Đồng Tháp giai đoạn 2021 - 2025

Thực hiện các chỉ đạo của Trung ương về Ứng phó sự cố, bảo đảm an toàn thông tin mạng (*kèm theo Phụ lục I*), Ủy ban nhân dân Tỉnh ban hành Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Đồng Tháp giai đoạn 2021 - 2025 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; khả năng thích ứng một cách chủ động, linh hoạt, giảm thiểu các nguy cơ mất an toàn thông tin trên mạng; đề ra các phương án ứng phó khi phát sinh sự cố mất an toàn thông tin mạng.

- Bảo đảm các nguồn lực và điều kiện cần thiết để triển khai kịp thời các phương án ứng cứu khẩn cấp sự cố an toàn thông tin mạng.

- Nâng cao nhận thức, kỹ năng về bảo đảm an toàn thông tin mạng cho cán bộ, công chức, viên chức và người dân.

2. Yêu cầu

- Căn cứ kết quả giám sát, khảo sát và đánh giá nguy cơ mất an toàn thông tin mạng của các hệ thống thông tin trong các cơ quan nhà nước trên địa bàn Tỉnh để đưa ra các phương án ứng phó phù hợp.

- Phương án đối phó, ứng cứu sự cố an toàn thông tin mạng phải đề ra các tiêu chí để kịp thời xác định tính chất, mức độ nghiêm trọng của sự cố khi có sự cố xảy ra.

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

II. NHIỆM VỤ TRIỂN KHAI

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

- Tuyên truyền, phổ biến Quyết định số 05/2017/QĐ-TTg ngày 16 tháng

3 năm 2017 và các văn bản quy phạm pháp luật về an toàn thông tin mạng.

- Triển khai các chương trình huấn luyện, diễn tập; phòng ngừa sự cố, giám sát phát hiện sớm sự cố; các điều kiện sẵn sàng ứng phó, ứng cứu, khắc phục sự cố.

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

(Chi tiết Phụ lục II kèm theo)

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

a) Tiếp nhận, phân tích, ứng cứu ban đầu và thông báo sự cố

- Tiếp nhận, xác minh sự cố.
- Triển khai các bước ưu tiên ứng cứu ban đầu.
- Triển khai lựa chọn phương án ứng cứu.
- Chỉ đạo xử lý sự cố *(nếu cần)*.
- Báo cáo sự cố.
- Điều phối công tác ứng cứu.

b) Triển khai ứng cứu, ngăn chặn và xử lý sự cố

c) Xử lý sự cố, gỡ bỏ mã độc và khôi phục hệ thống

- Xử lý sự cố, gỡ bỏ mã độc.
- Khôi phục hệ thống.
- Kiểm tra, đánh giá hệ thống thông tin.

d) Tổng kết, đánh giá

(Chi tiết Phụ lục III kèm theo)

III. KINH PHÍ THỰC HIỆN

Từ nguồn ngân sách nhà nước theo phân cấp, nguồn tài trợ, nguồn thu hợp pháp khác *(nếu có)*.

IV. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành Tỉnh; Ủy ban nhân dân huyện, thành phố

- Thủ trưởng các sở, ban, ngành, Chủ tịch Ủy ban nhân dân huyện, thành phố căn cứ nội dung Kế hoạch này, tình hình thực tế tại cơ quan, đơn vị và địa phương, ban hành Kế hoạch triển khai thực hiện.

- Bố trí cán bộ, công chức phụ trách công tác bảo đảm an toàn thông tin mạng tại cơ quan, đơn vị và địa phương; kịp thời thông báo về Sở Thông tin và Truyền thông khi có sự thay đổi cán bộ, công chức tham mưu công tác bảo đảm an toàn thông tin mạng.

- Phối hợp với cơ quan, đơn vị chủ trì thực hiện các nhiệm vụ được giao theo Kế hoạch này; chủ động xây dựng dự toán kinh phí hằng năm, gửi về Sở Thông tin và Truyền thông tổng hợp.

2. Sở Thông tin và Truyền thông

- Là cơ quan chuyên trách về ứng cứu sự cố an toàn thông tin mạng trên địa bàn Tỉnh, có trách nhiệm triển khai Kế hoạch ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn Tỉnh hằng năm; theo dõi, đôn đốc, phối hợp với các sở, ban, ngành Tỉnh, Ủy ban nhân dân huyện, thành phố trong việc triển khai thực hiện Kế hoạch này; định kỳ 6 tháng, một năm báo cáo kết quả thực hiện về Ủy ban nhân dân Tỉnh nắm.

- 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 tháng 9 năm 2017.

3. Sở Tài chính: Thẩm định dự toán kinh phí, tham mưu Ủy ban nhân dân Tỉnh bố trí ngân sách nhà nước để thực hiện Kế hoạch phù hợp khả năng ngân sách và theo đúng quy định hiện hành.

Trong quá trình triển khai thực hiện, nếu có khó khăn, vướng mắc vượt thẩm quyền, các cơ quan, đơn vị và địa phương phản ánh về Sở Thông tin và Truyền thông để tổng hợp, báo cáo Ủy ban nhân dân Tỉnh xem xét, quyết định./.

Nơi nhận:

- Bộ Thông tin và Truyền thông (b/c);
- CT và các PCT/UBND Tỉnh;
- Mục IV;
- Lãnh đạo VP/UBND Tỉnh;
- Lưu: VT, THVX. Thg

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

Huỳnh Minh Tuấn

Phụ lục I
CÁC VĂN BẢN CHỈ ĐẠO CỦA TRUNG ƯƠNG
(kèm theo Kế hoạch số: /KH-UBND ngày tháng năm 2021
của Ủy ban nhân dân Tỉnh)

1. Quyết định số 05/2017/QĐ-TTg ngày 16 tháng 3 năm 2017 của Thủ tướng Chính phủ về ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;
2. Quyết định số 1017/QĐ-TTg ngày 14 tháng 8 năm 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 đến năm 2020, định hướng đến năm 2025;
3. Chỉ thị số 14/CT-TTg ngày 07 tháng 6 năm 2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;
4. Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 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.

Phụ lục II
TRIỂN KHAI CÁC NHIỆM VỤ KHI CHƯA CÓ SỰ CỐ XẢY RA
(kèm theo Kế hoạch số: /KH-UBND ngày tháng năm 2021 của Ủy ban nhân dân Tỉnh)

Stt	Nhiệm vụ	Đơn vị chủ trì	Đơn vị phối hợp	Thời gian hoàn thành	Ghi chú
1	Tổ chức tuyên truyền, phổ biến trên các phương tiện thông tin đại chúng, tài liệu tuyên truyền, Cổng Thông tin điện tử Tỉnh, các trang thông tin điện tử của các sở, ban, ngành Tỉnh và Ủy ban nhân dân huyện, thành phố về Quyết định số 05/2017/QĐ-TTg và các văn bản quy phạm pháp luật về an toàn thông tin mạng.	Sở Thông tin và Truyền thông	Các sở, ban, ngành Tỉnh; UBND huyện, thành phố và các đơn vị có liên quan	Thường xuyên	
2	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; kỹ năng, nghiệp vụ phối hợp, ứng cứu, chống tấn công, xử lý mã độc, khắc phục sự cố.	Sở Thông tin và Truyền thông; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Đồng Tháp		Mỗi năm ít nhất 01 lần	
3	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	Sở Thông tin và Truyền thông; Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Đồng Tháp; đơn vị quản lý, vận hành hệ thống thông tin	Đơn vị quản lý, vận hành hệ thống thông tin, VNCERT; các đơn vị liên quan khác	Mỗi năm ít nhất 01 lần	
4	Trang bị, nâng cấp trang thiết bị, công cụ, phương tiện, 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, tham gia các hoạt động của mạng lưới ứng cứu sự cố			Hàng năm	
5	Tổ chức đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng của 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 nếu xảy ra sự cố; đánh giá về hiện trạng phương tiện, trang thiết bị, công cụ hỗ trợ, nhân lực, vật lực phục vụ đối phó, ứng cứu, khắc phục sự cố <i>(bao gồm của cả nhà thầu đã ký hợp đồng cung cấp dịch vụ nếu có)</i> .	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 Đồng Tháp; các nhà thầu cung cấp dịch vụ an toàn thông tin mạng <i>(nếu có)</i> ; các đơn vị liên quan khác.	Hàng năm	
6	Xây dựng phương án ứng phó, ứng cứu đối với một số tình huống sự cố cụ thể			Thường xuyên trong năm	

Phụ lục III
TRIỂN KHAI CÁC NHIỆM VỤ KHI CÓ SỰ CỐ XẢY RA
(kèm theo Kế hoạch số: /KH-UBND ngày tháng năm 2021 của Ủy ban nhân dân Tỉnh)

Stt	Nhiệm vụ	Đơn vị chủ trì	Đơn vị phối hợp	Ghi chú
1	Theo dõi, tiếp nhận, phân tích các cảnh báo, dấu hiệu sự cố có thể từ các nguồn bên trong và bên ngoài (<i>tổ chức ghi nhận, thu thập chứng cứ, xác định nguồn gốc sự cố</i>)	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 Đồng Tháp, VNCERT; các đơn vị liên quan khác	
2	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.			
3	Lựa chọn phương án ngăn chặn và xử lý sự cố; báo cáo, đề xuất chủ quản hệ thống thông tin			
4	Chỉ đạo cơ quan chuyên trách ứng cứu sự cố an toàn thông tin mạng trên địa bàn Tỉnh, triệu tập Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Đồng Tháp triển khai công tác ứng cứu, xử lý sự cố; chỉ đạo, phân công hoạt động phát ngôn, cung cấp thông tin.	Ban Chỉ đạo Chuyển đổi số tỉnh Đồng Tháp	Chủ quản hệ thống thông tin; VNCERT	
5	Báo cáo sự cố đến các tổ chức, cá nhân liên quan bên trong và bên ngoài cơ quan, tổ chức theo quy định tại Điều 9 Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 2017 và quy định nội bộ (<i>nếu có</i>)	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 Đồng Tháp; VNCERT; các đơn vị liên quan khác	
6	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 Đồng Tháp, VNCERT	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 Đồng Tháp; các đơn vị liên quan khác.	
7	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 tỉnh Đồng Tháp	Sở Thông tin và Truyền thông, VNCERT; các đơn vị liên quan khác	

Stt	Nhiệm vụ	Đơn vị chủ trì	Đơn vị phối hợp	Ghi chú
8	Gỡ bỏ các mã độc, phần mềm độc hại, khắc phục các điểm yếu an toàn thông tin của 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 tỉnh Đồng Tháp	Sở Thông tin và Truyền thông, VNCERT	
9	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 cho hệ thống thông tin.		Sở Thông tin và Truyền thông, Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Đồng Tháp, VNCERT	
10	Kiểm tra, đánh giá hoạt động của toàn bộ hệ thống thông tin sau khi khắc phục sự cố. Trường hợp hệ thống chưa hoạt động ổn định, cần tiếp tục tổ chức thu thập, xác minh lại nguyên nhân, xử lý dứt điểm, khôi phục hoạt động bình thường của hệ thống thông 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 Đồng Tháp, VNCERT; các đơn vị khác liên quan	
11	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 Chuyên đổi số tỉnh Đồng Tháp và VNCERT; đồng thời, 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.			Sở Thông tin và Truyền thông, Đội ứng cứu khẩn cấp sự cố an toàn thông tin mạng tỉnh Đồng Tháp, Ban Chỉ đạo Chuyên đổi số tỉnh Đồng Tháp, VNCERT