ỦY BAN NHÂN DÂN THÀNH PHỐ CẦN THƠ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số:149 /KH-UBND	*Cần Thơ, ngày 03 tháng 4 năm 2026*

KẾ HOẠCH
Ứng phó sự cố an toàn thông tin mạng trên địa bàn thành phố Cần Thơ

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; Nghị quyết số 71/NQ-CP ngày 01/4/2025 của Chính phủ sửa đổi, bổ sung cập nhật chương trình hành động của Chính phủ 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; 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; Kế hoạch số 224/KH-UBND ngày 31/12/2025 của Ủy ban nhân dân thành phố Cần Thơ về Chuyển đổi số thành phố Cần Thơ năm 2026; Ủy ban nhân dân (UBND) thành phố ban hành Kế hoạch ứng phó sự cố an toàn thông tin mạng trên địa bàn thành phố, 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 thành phố; bảo đảm khả năng thích ứng chủ động, linh hoạt và giảm thiểu các nguy cơ, đe dọa mất an toàn thông tin trên mạng; kịp thời khắc phục các tồn tại, lỗ hổng, điểm yếu nhằm phòng ngừa các sự cố tấn công mạng; đề ra các giải pháp ứng phó khi gặp sự cố an toàn thông tin mạng.

- Tạo chuyển biến mạnh mẽ trong nhận thức về an ninh mạng, an toàn thông tin đối với cán bộ, công chức, viên chức trong các cơ quan nhà nước của thành phố.

- Xây dựng, phát triển Đội Ứng cứu sự cố an toàn thông tin mạng có đầy đủ kiến thức, kỹ năng xử lý sự cố an toàn thông tin mạng đảm bảo linh hoạt, hiệu quả, phù hợp với yêu cầu thực tế.

- Đảm bảo 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

- Các hệ thống thông tin của các cơ quan, đơn vị, địa phương phải được đánh giá hiện trạng và khả năng bảo đảm an toàn thông tin mạng, dự báo các nguy cơ, sự cố, tấn công mạng có thể xảy ra để đưa ra phương án ứng phó, ứng cứu sự cố kịp thời, phù hợp.

- 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.

- 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 đảm bảo an toàn thông tin giữa các cơ quan nhà nước trên địa bàn thành phố; tăng cường sự phối hợp, hỗ trợ của cơ quan điều phối quốc gia về ứng cứu sự cố (VNCERT).

- 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.

II. CÁC QUY ĐỊNH CHUNG

1. Phạm vi và đối tượng

Ứng phó sự cố an ninh mạng, an toàn thông tin đối với hệ thống thông tin các cơ quan, đơn vị, địa phương, tổ chức chính trị - xã hội trên địa bàn thành phố Cần Thơ.

2. Nguyên tắc, phương châm ứng phó sự cố

- Tuân thủ các quy định pháp luật về điều phối, ứng cứu sự cố an ninh mạng, an toàn thông tin mạng.

- Chủ động, kịp thời, nhanh chóng, chính xác; phối hợp chặt chẽ và đồng bộ và hiệu quả giữa các cơ quan, đơn vị.

- Ứng cứu sự cố trước hết phải được thực hiện, xử lý bằng lực lượng tại chỗ và trách nhiệm chính của chủ quản hệ thống thông tin.

- Thông tin trao đổi trong mạng lưới phải được kiểm tra, xác thực đối tượng trước khi thực hiện các bước tác nghiệp tiếp theo.

- Bảo đảm bí mật thông tin khi tham gia, thực hiện các hoạt động ứng cứu cố theo yêu cầu của cơ quan điều phối quốc gia hoặc cơ quan, tổ chức, cá nhân gặp sự cố.

3. Các lực lượng tham gia ứng phó sự cố

- Các sở, ban, ngành, đoàn thể thành phố; UBND các xã, phường; các cơ quan, đơn vị, doanh nghiệp có liên qua.

- Đội Ứng cứu sự cố an toàn thông tin mạng thành phố Cần Thơ (cơ quan Thường trực là Công an thành phố).

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

- Doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (trường hợp thuê dịch vụ).

- Trong trường hợp cần thiết, mời các cơ quan chuyên trách của các bộ, ngành Trung ương có chức năng ứng cứu an ninh mạng, an toàn thông tin mạng cùng tham gia.

4. Chức năng, nhiệm vụ, trách nhiệm và cơ chế, quy trình phối hợp giữa các cơ quan, đơn vị

- Công an thành phố: Đơn vị chuyên trách về an toàn thông tin mạng của thành phố Cần Thơ; thực hiện chỉ đạo, tổ chức triển khai hoạt động ứng phó sự cố an toàn thông tin mạng và các nhiệm vụ khác khi xảy ra sự cố. Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an thành phố: Có trách nhiệm tổ chức quản lý, triển khai giám sát an toàn thông tin, cảnh báo về an toàn thông tin; là đầu mối điều phối kỹ thuật để xử lý thông tin vi phạm pháp luật trên không gian mạng theo quy định của pháp luật; tổ chức triển khai, kết nối chia sẻ thông tin với Trung tâm An ninh mạng quốc gia thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an.

- Đội Ứng cứu sự cố an toàn thông tin mạng thành phố: Lực lượng chính tham gia các hoạt động ứng cứu sự cố an toàn thông tin mạng; thực hiện nhiệm vụ theo Quy chế hoạt động của Đội; tham gia hoạt động ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia khi có yêu cầu từ Bộ Công an hoặc các bộ, ngành có liên quan.

- Trung tâm Giám sát, điều hành đô thị thông minh thành phố (thuộc Sở Khoa học và Công nghệ): Chịu trách nhiệm xây dựng, thực thi các quy định về an toàn bảo mật thông tin mạng, quản lý, khai thác và vận hành Trung tâm Dữ liệu; tham gia Đội Ứng cứu sự cố an toàn thông tin ninh mạng của thành phố; xử lý, ứng cứu các sự cố về an toàn thông tin, an ninh mạng xảy ra trên địa bàn thành phố Cần Thơ khi có yêu cầu của đơn vị điều phối.

- Các cơ quan, đơn vị, địa phương: Có trách nhiệm cử cán bộ, công chức, viên chức phụ trách an toàn thông tin tham gia Đội Ứng cứu sự cố an toàn thông tin mạng của thành phố khi xảy ra sự cố; phối hợp với đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng của thành phố trong công tác ứng phó, xử lý các sự cố.

- Doanh nghiệp cung cấp, xây dựng các hệ thống thông tin: Phối hợp với Công an thành phố, chủ quản hệ thống thông tin, đơn vị quản lý, vận hành hệ thống thông tin trong công tác ứng phó, xử lý các sự cố an toàn thông tin liên quan hệ thống thông tin do mình xây dựng hoặc cung cấp.

III. NỘI DUNG THỰC HIỆN

1. Đánh giá các nguy cơ, sự cố an toàn thông tin mạng

a) 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, tấn công mạng có thể xảy ra với các hệ thống thông tin và các đối tượng cần bảo vệ; 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 (bao gồm cả đơn vị cung cấp dịch vụ nếu có)

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

- Đơn vị phối hợp: Công an thành phố; Trung tâm Giám sát, điều hành đô thị thông minh thành phố Cần Thơ (Sở Khoa học và Công nghệ); các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (trường hợp thuê dịch vụ) và các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

b) Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng bảo mật đối với các hệ thống thông tin trong phạm vi quản lý; khắc phục các lỗ hổng, điểm yếu theo cảnh báo của cơ quan chức năng (thực hiện theo quy định tại Chỉ thị số 18/CT-TTg ngày 13/10/2022 của Thủ tướng Chính phủ)

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

- Đơn vị phối hợp: Công an thành phố; Trung tâm Giám sát, điều hành đô thị thông minh thành phố Cần Thơ (Sở Khoa học và Công nghệ); các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (trường hợp thuê dịch vụ) và các cơ quan, đơn vị khác có liên quan.

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

2. Phương án đối phó, ứng cứu đối với một số tình huống sự cố cụ thể

Đối với mỗi hệ thống thông tin, chương trình ứng dụng, các cơ quan, đơn vị, địa phương 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 của sự cố khi sự cố xảy ra. Việc xây dựng phương án đối phó, ứng cứu sự cố cần bảo đảm các nội dung:

a) Phương pháp, cách thức để xác định nhanh chóng, kịp thời nguyên nhân, nguồn gốc sự cố nhằm áp dụng phương án đối phó, ứng cứu, khắc phục sự cố phù hợp. Các trường hợp cụ thể:

- 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 thảm họa tự nhiên như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất an toàn thông tin mạng khác.

b) Phương án đối phó, khắc phục sự cố đối với một hoặc nhiều tình huống.

- 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 hệ thống.

- Tình huống sự cố do lỗi từ người dùng cuối trong quá trình khai thác, sử dụng hệ thống:

+ Chia sẻ thông tin, sử dụng chung tài khoản sai quy định;

+ Lưu mật khẩu mặc định trên trình duyệt, làm lộ, mất thông tin đăng nhập;

+ Không tuân thủ quy trình, quy chế, chính sách an toàn thông tin đã ban hành.

- Tình huống sự cố liên quan đến các thiên tai, thảm họa tự nhiên, như bão, lụt, động đất, hỏa hoạn và các sự cố gây mất an toàn thông tin mạng khác.

c) Công tác tổ chức, điều hành, phối hợp giữa các lực lượng, các tổ chức trong đối phó, ngăn chặn, ứng cứu, khắc phục sự cố

- Đơn vị chủ trì: Công an thành phố.

Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; các sở, ban, ngành, đoàn thể của thành phố; UBND các xã,

phường; Đội Ứng cứu sự cố an toàn thông tin mạng thành phố; Trung tâm Giám sát, điều hành đô thị thông minh thành phố Cần Thơ (Sở Khoa học và Công nghệ); các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

d) Phương án về nhân lực, trang thiết bị, 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

- Đơn vị chủ trì: Các sở, ban, ngành, đoàn thể thành phố; UBND các xã, phường.

- Đơn vị phối hợp: Công an thành phố; Đội Ứng cứu sự cố an toàn thông tin mạng thành phố; Trung tâm Giám sát, điều hành đô thị thông minh thành phố Cần Thơ (Sở Khoa học và Công nghệ); các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); các cơ quan, đơn vị khác có liên quan.

- Thời gian thực hiện: Thường xuyên.

3. Triển khai hoạt động thường trực, điều phối, xử lý, ứng cứu sự cố

a) Báo cáo sự cố an toàn thông tin mạng theo quy định tại Điều 11, Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ, Điều 9 Thông tư số 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ)

- Đơn vị thực hiện:

+ Đơn vị quản lý, vận hành hệ thống thông tin báo cáo cơ quan chủ quản hệ thống thông tin, Đội Ứng cứu sự cố an toàn thông tin mạng thành phố (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an thành phố); đồng gửi Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an.

+ Công an thành phố báo cáo Chủ tịch UBND thành phố, Cơ quan điều phối quốc gia và báo cáo Cơ quan thường trực và Ban Chỉ đạo quốc gia về ứng cứu sự cố.

- Thời gian thực hiện: Ngay khi xảy ra sự cố và được duy trì trong suốt quá trình ứng cứu sự cố.

b) Tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng theo quy định tại Điều 12 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Điều 10 Thông tư 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ)

- Đơn vị chủ trì: Công an thành phố; đơn vị quản lý, vận hành hệ thống thông tin (các cơ quan, đơn vị); Đội Ứng cứu sự cố an toàn thông tin mạng thành phố.

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; tổ chức, cá nhân gửi thông báo, báo cáo sự cố; các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); các cơ quan, đơn vị chức năng liên quan.

- Thời gian thực hiện: Ngay sau khi phát hiện sự cố hoặc nhận được thông báo, báo cáo sự cố của tổ chức, cá nhân.

c) Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường và nghiêm trọng theo quy định tại Điều 13 và Điều 14 Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Điều 11 Thông tư 20/2017/TT-BTTTT của Bộ trưởng Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ)

- Đơn vị chủ trì: Đội Ứng cứu sự cố an toàn thông tin mạng thành phố (cơ quan Thường trực là Công an thành phố).

- Đơn vị phối hợp: Các sở, ban, ngành, đoàn thể; UBND các xã, phường; đơn vị quản lý, vận hành hệ thống thông tin.

- Thời gian thực hiện: Thường xuyên.

4. Triển khai huấn luyện, diễn tập, phòng ngừa sự cố, giám sát phát hiện, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Xây dựng các nội dung, nhiệm vụ cụ thể cần triển khai nhằm phòng ngừa sự cố, giám sát phát hiện, huấn luyện, diễn tập, bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố. Đồng thời, cần đáp ứng đúng theo quy định tại Chỉ thị số 60/CT-BTTTT ngày 16/9/2021 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) về việc tổ chức triển khai diễn tập thực chiến bảo đảm an toàn thông tin mạng, bao gồm:

a) Triển khai các chương trình huấn luyện, diễn tập

Tổ chức diễn tập các phương án đối phó, ứng cứu sự cố tương ứng với các kịch bản, tình huống sự cố cụ thể; huấn luyện, diễn tập 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, diễn tập vùng, miền, quốc gia, quốc tế.

- Đơn vị chủ trì: Công an thành phố; Đội Ứng cứu sự cố an toàn thông tin mạng thành phố.

- Đơn vị phối hợp: Đơn vị quản lý, vận hành hệ thống thông tin, Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

b) Triển khai nhiệm vụ nhằm phòng ngừa sự cố và phát hiện sớm sự cố

Thực hiện nghiêm công tác giám sát, phát hiện sớm 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.

- Đơn vị chủ trì: Công an thành phố; đơn vị quản lý, vận hành hệ thống thông tin; Đội Ứng cứu sự cố an toàn thông tin mạng thành phố.

- Đơn vị phối hợp: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Thường xuyên.

c) Các nội dung, nhiệm vụ nhằm bảo đảm các điều kiện sẵn sàng đối phó, ứng cứu, khắc phục sự cố

Mua sắm, nâng cấp, gia hạn bản quyền trang thiết bị, phần mềm, công cụ, phương tiện phục vụ ứng cứu, khắc phục sự cố; chuẩn bị các điều kiện bảo đảm, dự phòng nhân lực, vật lực, 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, bộ phận 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 chủ trì: Công an thành phố phối hợp các sở, ban, ngành, đoàn thể thành phố; UBND các xã, phường.

- Đơn vị phối hợp: Các doanh nghiệp cung cấp dịch vụ an toàn thông tin mạng (nếu có); Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam thuộc Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; các cơ quan, đơn vị chức năng có liên quan.

- Thời gian thực hiện: Hàng năm.

IV. KINH PHÍ THỰC HIỆN

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

V. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành thành phố và UBND các xã, phường

- Căn cứ nội dung Kế hoạch này và tình hình thực tế tại cơ quan, đơn vị, địa phương xây dựng, ban hành Kế hoạch Ứng phó sự cố an toàn thông tin mạng, nội dung theo hướng dẫn tại Phụ lục 3 của Thông tư 20/2017/TT- BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) theo thẩm quyền quản lý và tổ chức triển khai các nhiệm vụ về ứng phó sự cố an toàn thông tin mạng theo đúng tiến độ, chất lượng, hiệu quả.

- Phân công lãnh đạo phụ trách; thành lập hoặc chỉ định bộ phận đầu mối; bố trí cán bộ, công chức, viên chức chuyên trách thực hiện công tác bảo đảm an ninh mạng, an toàn thông tin tại cơ quan, đơn vị trong phạm vi quản lý. Khi có sự thay đổi cán bộ, công chức, viên chức chuyên trách về an toàn thông tin mạng tại cơ quan, đơn vị hoặc đang là thành viên tham gia Đội Ứng cứu sự cố an toàn thông tin mạng của thành phố thì đơn vị kịp thời thông báo về Công an thành phố qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao.

- 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 và lĩnh vực quản lý. Xây dựng nội dung, lập dự toán kinh phí thực hiện các nhiệm vụ về ứng phó sự cố, bảo đảm an toàn thông tin của cơ quan, đơn vị mình hàng năm để tổ chức triển khai thực hiện, tránh chồng chéo, lãng phí.

- Thực hiện đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và 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).

- Định kỳ (06 tháng, 01 năm) hoặc đột xuất, các đơn vị báo cáo tình hình ứng phó sự cố, bảo đảm an ninh mạng, an toàn thông tin trong phạm vi quản lý về Công an thành phố để tổng hợp báo cáo cấp trên theo quy định.

- Cử cán bộ tham gia đầy đủ các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn về ứng cứu sự cố, 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 mạng.

- Tổ chức tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn, các hoạt động liên quan đến đảm bảo an ninh mạng của thành phố, của cơ quan, đơn vị trên các Trang/Cổng thông tin điện tử, các phương tiện thông tin đại chúng: nội dung của Luật An an toàn thông tin mạng; Nghị định số 85/2016/NĐ-CP; Thông tư số 12/2022/TT-BTTTT; các Công điện, Chỉ thị của Thủ tướng Chính phủ và các Chỉ thị, văn bản của Bộ Công an, Bộ Khoa học và Công nghệ.

2. Công an thành phố

- Hằng năm tham mưu UBND thành phố ban hành Quyết định thành lập, kiện toàn Đội Ứng cứu sự cố an toàn thông tin mạng cho phù hợp với tình hình đảm bảo an toàn thông tin mạng trên địa bàn thành phố.

- Thực hiện trách nhiệm, quyền hạn của đơn vị chuyên trách ứng cứu sự cố an toàn thông tin mạng theo Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ Thông tin và Truyền thông (nay là Bộ Khoa học và Công nghệ) và Quyết định số 2214/QĐ-UBND ngày 04/11/2025 của UBND thành phố Cần Thơ.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát, hướng dẫn công tác bảo đảm an toàn thông tin định kỳ hàng năm hoặc theo chỉ đạo của Chủ tịch UBND thành phố đối với các cơ quan nhà nước trên địa bàn thành phố.

- 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 Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và hướng dẫn tại 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).

- Định kỳ (06 tháng, 01 năm) hoặc đột xuất, tổng hợp báo cáo kết quả thực hiện ứng phó sự cố, bảo đảm an ninh mạng, an toàn thông tin trên địa bàn thành phố gửi Chủ tịch UBND thành phố, Bộ Công an theo quy định.

- Xây dựng nội dung, lập dự toán kinh phí bảo đảm cho hoạt động của Đội Ứng cứu sự cố an toàn thông tin mạng của thành phố.

3. Sở Khoa học và Công nghệ thành phố

- Nghiên cứu, cập nhập các giải pháp quản lý, vận hành hệ thống thông tin tại Trung tâm Dữ liệu thành phố; hướng dẫn các đơn vị truy cập, khai thác các hệ thống thông tin dùng chung của thành phố bảo đảm đúng quy định, đạt hiệu quả; ban hành, sửa đổi, bổ sung các quy chế, quy trình khai thác hệ thống; chủ động phối hợp với Công an thành phố duy trì giám sát, kịp thời phát hiện, xử lý khắc phục các điểm yếu, lỗ hổng bảo mật và triển khai các biện pháp phòng chống, ngăn chặn tấn công mạng, bảo đảm hệ thống thông tin vận hành thông suốt, ổn định.

- Trao đổi, chia sẻ kịp thời với Công an thành phố (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) về thông tin liên quan đến sự cố mất an toàn thông tin mạng hệ thống thông tin tập trung, dùng chung của thành phố để chủ động phối hợp xử lý, ứng cứu khi cần thiết.

- 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 thành phố khi có yêu cầu của đơn vị điều phối.

- Phối hợp các cơ quan, đơn vị, địa phương triển khai thực hiện hiệu quả công tác tuyên truyền, phổ biến pháp luật và an toàn thông tin, an ninh mạng.

4. Sở Tài chính thành phố

Căn cứ khả năng cân đối của ngân sách địa phương, phối hợp với các cơ quan, đơn vị có liên quan tổng hợp, tham mưu UBND thành phố bố trí kinh phí để thực hiện Kế hoạch theo quy định của Luật Ngân sách nhà nước và các văn bản hướng dẫn liên quan.

Trong quá trình thực hiện nếu có khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương báo cáo kịp thời về UBND thành phố (qua Công an thành phố (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao)) để được chỉ đạo, giải quyết theo quy định. Giao Công an thành phố chủ trì, giúp Chủ tịch UBND thành phố theo dõi, hướng dẫn, kiểm tra, đôn đốc việc thực hiện và tổng hợp báo cáo theo quy định./.

Nơi nhận:
- Cục A05, Bộ Công an;
- TT: Thành ủy, HĐND TP;
- CT, PCT UBND TP;
- Sở, ban, ngành TP;
- Các doanh nghiệp cung cấp dịch vụ CNTT, viễn thông, internet trên địa bàn thành phố;
- UBND xã, phường;
- VP UBND TP (2E)
- Lưu: VT, NC.

CHỦ TỊCH

Trương Cảnh Tuyên