BỘ CÔNG AN **CÔNG AN TP CẦN THƠ**	**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: /TTr-CATP-PANM	*Cần Thơ, ngày tháng 12 năm 2025*

DỰ THẢO

TỜ TRÌNH

Dự thảo Quyết định ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ

Kính gửi: Ủy ban nhân dân thành phố Cần Thơ

Thực hiện quy định của Luật Ban hành văn bản quy phạm pháp luật năm 2025 (được sửa đổi, bổ sung năm 2025), Công an thành phố kính trình Ủy ban nhân nhân thành phố dự thảo Quyết định ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ, cụ thể như sau:

I. SỰ CẦN THIẾT BAN HÀNH VĂN BẢN

1. Cơ sở chính trị, pháp lý

- Căn cứ Luật Tổ chức chính quyền địa phương số 72/2025/QH15;

- Căn cứ Luật An toàn thông tin mạng số 86/2015/QH13;

- Căn cứ Luật An ninh mạng số 24/2018/QH14;

- Căn cứ Luật Dữ liệu số 60/2024/QH15;

- Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Căn cứ Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ Quy định chi tiết một số điều của Luật An ninh mạng số 86/2015/QH13;

- Căn cứ Nghị định số 147/2024/NĐ-CP ngày 09 tháng 11 năm 2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng;

- Căn cứ Thông tư số 20/2017/TT-BTTTT ngày 12 tháng 9 năm 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;

- Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15 tháng 11 năm 2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin;

- Căn cứ Thông tư số 12/2022/TT-BTTTT ngày 12 tháng 8 năm 2022 của 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 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

2. Cơ sở thực tiễn

Thực hiện chỉ đạo của Ban Chấp hành Trung ương, Bộ Chính trị, Chính phủ, Thủ tướng Chính phủ về việc chuyển giao nhiệm vụ quản lý nhà nước về an toàn, an ninh thông tin mạng từ ngành Thông tin và Truyền thông về lực lượng Công an, theo đó, từ ngày 01/3/2025, Công an 03 địa phương: thành phố Cần Thơ, tỉnh Hậu Giang và tỉnh Sóc Trăng đã tiếp nhận nhiệm vụ quản lý nhà nước về an toàn, an ninh thông tin mạng từ Sở Thông tin và Truyền thông (cũ) của 03 địa phương: thành phố Cần Thơ, tỉnh Hậu Giang và tỉnh Sóc Trăng.

Đồng thời, căn cứ khoản 19 Điều 1 Nghị quyết số 202/2025/QH15 ngày 12 tháng 6 năm 2025 của Quốc hội về việc sắp xếp đơn vị hành chính cấp tỉnh quy định:

*"**Điều 1. Sắp xếp đơn vị hành chính cấp tỉnh***

...

19. Sắp xếp toàn bộ diện tích tự nhiên, quy mô dân số của thành phố Cần Thơ, tỉnh Sóc Trăng và tỉnh Hậu Giang thành thành phố mới có tên gọi là thành phố Cần Thơ.".

Căn cứ điểm b khoản 2 Điều 54 Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15 được sửa đổi, bổ sung bởi Luật số 87/2025/QH15 quy định:

*"**Điều 54. Hiệu lực về không gian***

...

b) Trường hợp nhiều đơn vị hành chính được nhập thành một đơn vị hành chính mới cùng cấp thì văn bản quy phạm pháp luật của Hội đồng nhân dân, Ủy ban nhân dân, Chủ tịch Ủy ban nhân dân của đơn vị hành chính được nhập tiếp tục có hiệu lực trong phạm vi đơn vị hành chính đó cho đến khi Hội đồng nhân dân, Ủy ban nhân dân, Chủ tịch Ủy ban nhân dân của đơn vị hành chính mới ban hành văn bản hành chính để quyết định áp dụng hoặc bãi bỏ văn bản quy phạm pháp luật của Hội đồng nhân dân, Ủy ban nhân dân, Chủ tịch Ủy ban nhân dân của đơn vị hành chính được nhập hoặc ban hành văn bản quy phạm pháp luật mới.".

Ngày 28 tháng 8 năm 2025, Ủy ban nhân dân thành phố Cần Thơ đã ban hành Quyết định số 933/QĐ-UBND về bãi bỏ các Quyết định do Ủy ban nhân dân thành phố Cần Thơ, tỉnh Sóc Trăng, tỉnh Hậu Giang ban hành trước sắp xếp đơn vị hành chính, theo đó đã bãi bỏ Quyết định số 10/2013/QĐ-UBND ngày 08 tháng 4 năm 2013 của Ủy ban nhân dân tỉnh Sóc Trăng về ban hành Quy chế đảm bảo an toàn, an ninh thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Sóc Trăng.

Bên cạnh đó, thời gian qua, việc áp dụng các quy định của pháp luật về đảm bảo an toàn, an ninh thông tin chưa thống nhất như: Ủy ban nhân dân thành phố Cần Thơ ban hành văn bản hành chính đối với công tác đảm bảo an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ (*Quyết định số 2945/QĐ-UBND ngày 09 tháng 10 năm 2015)*, trong khi Ủy ban nhân dân tỉnh Hậu Giang (cũ), Sóc Trăng (cũ) ban hành văn bản quy phạm pháp luật; Quyết định của chính quyền địa phương (cũ) ban hành chưa được rà soát bãi bỏ (Quyết định số 48/2024/QĐ-UBND ngày 22 năm 11 năm 2024 của Ủy ban nhân dân tỉnh Hậu Giang ban hành Quy chế bảo đảm an toàn thông tin mạng trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn tỉnh Hậu Giang).... Đồng thời, sau sắp xếp đơn vị hành chính, tên gọi của một số cơ quan nhà nước đã có sự thay đổi hoặc không còn sử dụng; một số chức năng, nhiệm vụ được chuyển giao từ cơ quan này sang cơ quan khác để phù hợp với tổ chức, bộ máy mới nên một số quy định về đảm bảo an toàn, an ninh thông tin do chính quyền địa phương cũ ban hành đã không còn phù hợp với mô hình chính quyền địa phương hai cấp và tình hình thực tiễn công tác đảm bảo an ninh, trật tự trên địa bàn thành phố Cần Thơ (mới).

Từ những cơ sở pháp lý và vấn đề thực tiễn phát sinh nêu trên, để công tác quản lý nhà nước về an toàn, an ninh thông tin mạng trên địa bàn thành phố Cần Thơ được thống nhất, đồng bộ, hiệu quả sau khi sắp xếp chính quyền địa phương hai cấp thì việc rà soát, xây dựng Quyết định ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ là cần thiết.

II. MỤC ĐÍCH BAN HÀNH, QUAN ĐIỂM XÂY DỰNG QUYẾT ĐỊNH

1. Mục đích

- Thể chế hóa quan điểm, chủ trương của Đảng, Nhà nước về bảo đảm an ninh, an toàn thông tin mạng, đặc biệt là trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước.

- Xây dựng cơ sở pháp lý vững chắc, đồng bộ, hiệu quả về bảo đảm an ninh, an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước trên địa bàn thành phố Cần Thơ.

- Tăng cường công tác quản lý, giám sát, phát hiện và xử lý sự cố an ninh, an toàn thông tin mạng.

- Bảo đảm an toàn dữ liệu, phòng chống tấn công mạng, bảo vệ hệ thống thông tin phục vụ chuyển đổi số của thành phố Cần Thơ.

2. Quan điểm xây dựng dự thảo văn bản

- Tuân thủ Hiến pháp, bảo đảm tính thống nhất, đồng bộ trong hệ thống pháp

luật; bảo đảm các quy định của Quyết định được cụ thể và có tính khả thi cao.

- Bảo đảm đồng bộ với hệ thống pháp luật về an toàn thông tin, an ninh mạng, dữ liệu số.

- Trách nhiệm giữa người đứng đầu cơ quan, cán bộ kỹ thuật và đơn vị cung cấp dịch vụ CNTT.

- Tăng cường vai trò điều phối, giám sát và ứng cứu sự cố của Công an thành phố.

- Đặt công tác an toàn thông tin song hành cùng quá trình chuyển đổi số.

III. QUÁ TRÌNH XÂY DỰNG QUYẾT ĐỊNH

Quá trình xây dựng dự thảo Quyết định ban hành Quy chế bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin của các cơ quan nhà nước thuộc Ủy ban nhân dân thành phố Cần Thơ, Công an thành phố tuân thủ đúng quy định của Luật Ban hành văn bản quy phạm pháp luật số 64/2025/QH15 được sửa đổi, bổ sung bởi Luật số 87/2025/QH15 và các văn bản hướng dẫn thi hành, cụ thể:

1. Thực hiện Công văn số 2918/UBND-NC ngày 12/12/2025 của Ủy ban nhân dân thành phố Cần Thơ về việc chấp thuận xây dựng Quyết định của Ủy ban nhân dân thành phố, Công an thành phố đã xây dựng dự thảo Tờ trình, dự thảo Quyết định và Bảng so sánh, thuyết minh nội dung dự thảo Quyết định.

2. Lấy ý kiến của các Sở, ban, ngành, địa phương có liên quan và ý kiến phản biện xã hội; đăng tải dự thảo Quyết định trên Cổng thông tin điện tử Công an thành phố.

3. Tổng hợp tiếp thu, giải trình các ý kiến góp ý, phản biện xã hội và hoàn thiện hồ sơ dự thảo Quyết định gửi Sở Tư pháp thẩm định.

4. Tổng hợp tiếp thu, giải trình ý kiến thẩm định và chỉnh lý, hoàn thiện dự thảo Quyết định.

IV. BỐ CỤC VÀ NỘI DUNG CƠ BẢN CỦA DỰ THẢO VĂN BẢN

1. Phạm vi điều chỉnh, đối tượng áp dụng

a) Phạm vi điều chỉnh (Điều 1)

Quy chế này quy định các nội dung liên quan đến bảo đảm an toàn thông tin trong hoạt động ứng dụng công nghệ thông tin (CNTT) của các cơ quan nhà nước trên địa bàn thành phố Cần Thơ *(sau đây gọi tắt là cơ quan, đơn vị)*.

b) Đối tượng áp dụng (Điều 2)

- Các cơ quan nhà nước thành phố Cần Thơ, bao gồm: các sở, ban, ngành, các đơn vị sự nghiệp trực thuộc UBND thành phố; UBND các xã, phường và các đơn vị trực thuộc; các tổ chức chính trị - xã hội.

- Các tổ chức, cá nhân liên quan đến an toàn thông tin mạng trong các cơ quan nhà nước nêu tại Khoản 1 Điều này.

2. Bố cục của dự thảo văn bản

Dự thảo Quy chế gồm 04 chương, 30 điều và 03 phụ lục biểu mẫu báo cáo, xử lý sự cố, cụ thể:

- Chương I: Quy định chung (từ Điều 1 đến Điều 7);

- Chương II: Bảo đảm an toàn thông tin trong thiết kế, xây dựng hệ thống thông tin (từ Điều 7 đến Điều 11);

- Chương III: Bảo đảm an toàn thông tin trong vận hành, sử dụng (từ Điều 12 đến Điều 26);

- Chương IV: Tổ chức thực hiện (từ Điều 27 đến Điều 30).

3. Một số nội dung cơ bản

a) Nguyên tắc bảo đảm an toàn thông tin mạng (Điều 4)

- Việc bảo đảm an toàn, an ninh thông tin là yêu cầu bắt buộc trong quá trình thiết kế, xây dựng, vận hành, nâng cấp, sử dụng và hủy bỏ trong ứng dụng công nghệ thông tin (CNTT) của cơ quan nhà nước; bảo đảm an toàn thông tin mạng (ATTTM) được thực hiện một cách tổng thể, đồng bộ, tập trung, xuyên suốt trong các hoạt động đầu tư, mua sắm, nâng cấp các giải pháp, vận hành, bảo trì, ngừng sử dụng hạ tầng, HTTT, phần mềm, dữ liệu. Có sự dùng chung, chia sẻ tài nguyên để tối ưu hiệu năng, tránh đầu tư thừa, trùng lặp.

- Việc thực hiện các phương pháp bảo đảm an toàn, an ninh thông tin phải tuân theo quy định của Luật An toàn thông tin mạng, Nghị định số 85/2016/NĐ-CP và Thông tư số 12/2022/TT-BTTTT.

- Trách nhiệm bảo đảm ATTTM gắn với trách nhiệm của người đứng đầu cơ quan, đơn vị và cá nhân trực tiếp liên quan.

- Trường hợp có quy định khác tại văn bản quy phạm pháp luật, quyết định của cấp có thẩm quyền cao hơn thì áp dụng quy định tại văn bản đó.

- Thông tin thuộc Danh mục bí mật nhà nước được bảo vệ theo quy định của pháp luật về bảo vệ bí mật nhà nước.

- Bố trí nguồn lực phù hợp với quy mô, điều kiện của cơ quan, đơn vị nhằm thực hiện tốt nhất công tác bảo đảm an toàn, an ninh thông tin.

b) Những hành vi bị nghiêm cấm theo quy định của pháp luật (Điều 5)

- Các hành vi bị nghiêm cấm về an toàn, an ninh thông tin mạng quy định tại Điều 7 Luật An toàn thông tin mạng số 86/2015/QH13, Điều 8 Luật An ninh mạng số 24/2018/QH14, Điều 5 Luật Bảo vệ bí mật nhà nước số 29/2018/QH14.

- Các hành vi bị cấm trong quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng quy định tại Điều 8 Luật số 24/2018/QH14, Điều 9 Luật Viễn thông ngày 24 tháng 11 năm 2023, quyền và nghĩa vụ của người sử dụng Internet theo quy định tại Điều 7 Nghị định số 147/2024/NĐ-CP ngày 09 tháng 11 năm 2024 của Chính phủ về quản lý, cung cấp, sử dụng dịch vụ Internet và thông tin trên mạng.

- Tự ý đấu nối thiết bị mạng, thiết bị cấp phát địa chỉ mạng, thiết bị phát sóng như điểm truy cập mạng không dây của cá nhân vào mạng nội bộ; tự ý thay đổi các cài đặt hệ thống mạng của cơ quan, đơn vị.

- Tự ý thay đổi, gỡ bỏ biện pháp an toàn thông tin cài đặt trên thiết bị CNTT phục vụ công việc; tự ý thay thế, lắp mới, tráo đổi thành phần của máy tính phục vụ công việc.

- Cản trở hoạt động cung cấp dịch vụ của hệ thống thông tin; ngăn chặn việc truy nhập đến thông tin của cơ quan, đơn vị và cá nhân khác trên môi trường mạng, trừ trường hợp pháp luật cho phép.

- Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của cơ quan, đơn vị và cá nhân khác trên môi trường mạng.

- Các hành vi khác làm mất an toàn, bí mật thông tin của cơ quan, đơn vị và cá nhân khác được trao đổi, truyền đưa, lưu trữ trên môi trường mạng.

c) Đầu mối liên hệ, ứng cứu sự cố an toàn thông tin mạng (Điều 6)

- Đầu mối ứng cứu sự cố ATTTM trong cơ quan nhà nước thành phố Cần Thơ: Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao Công an thành phố Cần Thơ, thư điện tử: anninhmang.catpcantho@cantho.gov.vn, số điện thoại: 0693.672.605,.

- Đầu mối liên hệ, phối hợp với các cơ quan, tổ chức ngoài thành phố trong công tác hỗ trợ điều phối xử lý sự cố ATTTM: Trung tâm Ứng cứu khẩn cấp không gian mạng Việt Nam (VNCERT), thư điện tử: report@vncert.vn, số điện thoại 0692.205.199.

d) Thiết kế an toàn hệ thống thông tin (HTTT) (Điều 8)

- Có tài liệu mô tả quy mô, phạm vi và đối tượng sử dụng, khai thác, quản lý vận hành HTTT.

- Có tài liệu mô tả thiết kế và các thành phần của HTTT.

- Có tài liệu mô tả phương án bảo đảm an toàn thông tin theo cấp độ.

- Có tài liệu mô tả phương án lựa chọn giải pháp công nghệ bảo đảm an toàn thông tin.

- Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.

đ) Phát triển phần mềm thuê khoán (Điều 9)

- Có biên bản, hợp đồng và các cam kết đối với bên thứ ba các nội dung liên quan đến việc phát triển phần mềm thuê khoán.

- Yêu cầu các nhà phát triển cung cấp mã nguồn phần mềm.

- Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng.

- Kiểm tra, đánh giá an toàn thông tin, trước khi đưa vào sử dụng.

e) Xác định cấp độ và phương án bảo đảm an toàn cho các HTTT (Điều 11)

- Chủ quản HTTT thực hiện phân loại, xác định cấp độ HTTT, giao đơn vị vận hành HTTT xây dựng hồ sơ đề xuất bảo đảm an toàn HTTT theo cấp độ trong đó phải có phương án bảo đảm an toàn HTTT phù hợp với cấp độ của HTTT và đáp ứng yêu cầu quy định tại Nghị định số 85/2016/NĐ-CP, Thông tư số 12/2022/TT-BTTTT, tiêu chuẩn TCVN 11930:2017, các tiêu chuẩn, quy chuẩn kỹ thuật khác và chính sách ATTTM của cơ quan ngành dọc Trung ương (nếu có).

- HTTT đang vận hành trong các cơ quan nhà nước hoặc HTTT khi được đầu tư xây dựng mới hoặc mở rộng, nâng cấp phải được thẩm định, phê duyệt hồ sơ cấp độ và triển khai đầy đủ các phương án bảo đảm ATTT theo cấp độ tương ứng.

- Các HTTT đang vận hành trong các cơ quan nhà nước phải được kiểm tra đánh giá định kỳ theo Hồ sơ đề xuất cấp độ đã phê duyệt và bố trí kinh phí để nâng cấp, vá lỗi.

g) Quản lý trang thiết bị ứng dụng công nghệ thông tin trong hoạt động của cơ quan, đơn vị (Điều 12)

- Giao, gắn trách nhiệm cho cá nhân hoặc tập thể quản lý, sử dụng trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị.

- Cơ quan, đơn vị quy định các quy tắc sử dụng, giữ gìn bảo vệ trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị trong các trường hợp như: mang ra khỏi cơ quan, trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị liên quan đến dữ liệu nhạy cảm, cài đặt và cấu hình.

- Trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị khi thay đổi mục đích sử dụng hoặc thanh lý thì cơ quan, đơn vị phải thực hiện các biện pháp xóa, tiêu hủy dữ liệu đó bảo đảm không có khả năng phục hồi. Trường hợp không thể tiêu hủy được dữ liệu, đơn vị phải thực hiện tiêu hủy cấu phần lưu trữ dữ liệu trên trang thiết bị ứng dụng CNTT trong hoạt động cơ quan, đơn vị đó.

- Thiết bị tính toán có bộ phận lưu trữ hoặc thiết bị lưu trữ khi mang đi bảo

hành, bảo dưỡng, sửa chữa bên ngoài hoặc ngừng sử dụng phải tháo bộ phận lưu trữ khỏi thiết bị hoặc xóa thông tin, dữ liệu lưu trữ trên thiết bị (trừ trường hợp để khôi phục dữ liệu).

- Cơ quan, đơn vị có trách nhiệm xây dựng quy trình bảo dưỡng, bảo trì và hướng dẫn cách sử dụng, quản lý, vận hành hệ thống hạ tầng kỹ thuật của đơn vị; thực hiện quản lý, vận hành và định kỳ kiểm tra, sửa chữa, bảo trì thiết bị (bao gồm thiết bị dự phòng).

h) Bảo đảm ATTTM khi sử dụng máy tính (Điều 15)

- Máy tính dùng để soạn thảo tài liệu mật thực hiện theo các quy định về bảo vệ bí mật nhà nước.

- Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật cơ sở dữ liệu cho phần mềm; khi phát hiện bất kỳ dấu hiệu nào liên quan đến việc bị nhiễm mã độc trên máy tính phải tắt máy và báo trực tiếp cho bộ phận phụ trách về ATTTM để được xử lý kịp thời.

- Cá nhân chỉ cài đặt phần mềm hợp lệ; không được tự ý cài đặt hoặc gỡ bỏ các phần mềm khi chưa có sự đồng ý của bộ phận phụ trách về ATTTM; thường xuyên cập nhật phần mềm và hệ điều hành.

- Chỉ truy cập vào các trang/cổng thông tin điện tử, ứng dụng trực tuyến tin cậy và các thông tin phù hợp với chức năng, trách nhiệm, quyền hạn của mình; có trách nhiệm bảo mật tài khoản truy cập thông tin, không chia sẻ mật khẩu, thông tin cá nhân với người khác.

- Không được sử dụng máy tính của cơ quan nhà nước để thâm nhập bất hợp pháp vào các mạng máy tính khác.

- Thường xuyên thay đổi mật khẩu truy cập HTTT, tối thiểu 03 tháng/lần. Khuyến khích đặt mật khẩu theo nguyên tắc: mật khẩu có tối thiểu 08 ký tự bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt.

i) Quản lý an toàn máy chủ và ứng dụng (Điều 18)

- Quản lý, vận hành hoạt động bình thường của hệ thống.

- Cập nhật, sao lưu dự phòng và khôi phục sau khi xảy ra sự cố.

- Truy cập và quản lý cấu hình hệ thống.

- Thường xuyên nâng cấp, cập nhật bản vá lỗ hổng bảo mật đối với các nền tảng ảo hóa, nền tảng ứng dụng, hệ điều hành để đáp ứng được yêu cầu bảo đảm an toàn thông tin.

k) Quản lý an toàn dữ liệu (Điều 19)

- Yêu cầu an toàn đối với phương pháp mã hóa.

- Phân loại, quản lý và sử dụng khóa bí mật và dữ liệu mã hóa.

- Cơ chế mã hóa và kiểm tra tính nguyên vẹn của dữ liệu không được sử dụng không được tồn tại điểm yếu an toàn thông tin ở mức cao do các tổ chức quốc tế hoặc Bộ Thông tin và Truyền thông công bố.

- Trao đổi dữ liệu qua môi trường mạng và phương tiện lưu trữ phải được mã hóa đáp ứng yêu cầu ở trên.

- Cập nhật đồng bộ thông tin, dữ liệu giữa hệ thống sao lưu dự phòng chính và hệ thống phụ phải được đồng bộ theo thời gian thực.

- Định kỳ hàng tháng hoặc khi có thay đổi cấu hình trên hệ thống thực hiện quy trình sao lưu dự phòng: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu; dữ liệu, thông tin nghiệp vụ và các thông tin, dữ liệu quan trọng khác trên HTTT.

l) Quản lý phòng chống mã độc (Điều 20)

- Cài đặt, cập nhật, sử dụng phần mềm phòng chống mã độc; dò quét, kiểm tra phần mềm độc hại trên máy tính, máy chủ và thiết bị di động.

- Cài đặt, sử dụng phần mềm trên máy tính, thiết bị di động và việc truy cập các trang thông tin trên mạng.

- Gửi nhận tập tin qua môi trường mạng và các phương tiện lưu trữ di động phải thực hiện qua kênh kết nối an toàn sử dụng giao thức mã hóa, xác thực không được tồn tại điểm yếu an toàn thông tin ở mức cao do các tổ chức quốc tế hoặc Bộ Thông tin và Truyền thông công bố.

- Định kỳ hàng năm thực hiện kiểm tra và dò quét phần mềm độc hại trên toàn bộ hệ thống; thực hiện kiểm tra và xử lý phần mềm độc hại khi phát hiện dấu hiệu hoặc cảnh báo về dấu hiệu phần mềm độc hại xuất hiện trên hệ thống.

m) Quản lý giám sát an toàn hệ thống thông tin (Điều 21)

- Quản lý, vận hành hoạt động của hệ thống giám sát.

- Đối tượng giám sát bao gồm tối thiểu bao gồm: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ.

- Kết nối và gửi nhật ký hệ thống từ đối tượng giám sát về hệ thống giám sát.

- Truy cập và quản trị hệ thống giám sát chỉ được thực hiện từ vùng mạng quản trị; trường hợp truy cập và quản trị từ mạng bên ngoài thì phải thông qua kênh kết nối VPN.

- Loại thông tin cần được giám sát bao gồm tối thiểu các loại sau: Thông tin giám sát lớp mạng, lớp máy chủ, lớp ứng dụng, cơ sở dữ liệu và thiết bị đầu cuối.

- Lưu trữ và bảo vệ thông tin giám sát phải được lưu trữ tập trung đầy đủ các

loại thông tin tại khoản 5 Điều này theo thời gian thực.

- Toàn bộ thành phần trong hệ thống giám sát, máy chủ, thiết bị hệ thống và ứng dụng phải được đồng bộ thời gian.

- Bộ phận giám sát thực hiện giám sát giám sát an toàn HTTT 24/7 để thực hiện theo dõi, giám sát và cảnh báo sự cố phát hiện được trên HTTT.

n) Quản lý điểm yếu an toàn thông tin (Điều 22)

- Quản lý thông tin các thành phần có trong HTTT có khả năng tồn tại điểm yếu an toàn thông tin: thiết bị hệ thống, hệ điều hành, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống nếu có.

- Quản lý, cập nhật nguồn cung cấp điểm yếu an toàn thông tin; phân nhóm và mức độ của điểm yếu cho các thành phần trong HTTT đã xác định

- Cơ chế phối hợp với các nhóm chuyên gia, bên cung cấp dịch vụ hỗ trợ trong việc xử lý, khắc phục điểm yếu an toàn thông tin

- Kiểm tra, đánh giá và xử lý điểm yếu ATTTM cho thiết bị hệ thống, máy chủ, dịch vụ trước khi đưa vào sử dụng.

- Định kỳ hàng năm kiểm tra, đánh giá điểm yếu an toàn thông tin cho toàn bộ HTTT; thực hiện quy trình kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin khi có thông tin hoặc nhận được cảnh báo về điểm yếu an toàn thông tin đối với thành phần cụ thể trong HTTT.

o) Quản lý sự cố an toàn thông tin mạng (Điều 23)

- Nguyên tắc ứng cứu sự cố:

- Cơ quan nhà nước xây dựng phương án quản lý sự cố ATTTM bao gồm các nội dung sau:

Phân nhóm sự cố an toàn thông tin mạng theo quy định tại Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ ngày 16/3/2017 quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia; xây dựng phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng, ứng phó sự cố an toàn thông tin mạng;

Phương án tiếp nhận, phát hiện, phân loại và xử lý ban đầu sự cố an toàn thông tin mạng;

Kế hoạch ứng phó sự cố an toàn thông tin mạng;

Giám sát, phát hiện và cảnh báo sự cố an toàn thông tin;

Quy trình ứng cứu sự cố an toàn thông tin mạng thông thường;

Quy trình ứng cứu sự cố an toàn thông tin mạng nghiêm trọng;

Cơ chế phối hợp với Đội Ứng cứu sự cố ATTTM thành phố, cơ quan chức năng trong và ngoài thành phố, các nhóm chuyên gia, bên thứ ba trong việc xử lý, khắc phục sự cố an toàn thông tin.

- Phương án Quản lý sự cố an toàn thông tin phải được ban hành cùng Quy chế bảo đảm an toàn thông tin trước khi đưa hệ thống vào vận hành, khai thác.

- Định kỳ hàng năm tổ chức diễn tập phương án xử lý sự cố an toàn thông tin.

V. NHỮNG NỘI DUNG BỔ SUNG MỚI SO VỚI DỰ THẢO VĂN BẢN GỬI THẨM ĐỊNH (NẾU CÓ)*: không.

VI. DỰ KIẾN NGUỒN LỰC, ĐIỀU KIỆN BẢO ĐẢM CHO VIỆC THI HÀNH VĂN BẢN VÀ THỜI GIAN TRÌNH BAN HÀNH

- Dự kiến nguồn lực: từ ngân sách nhà nước trong dự toán chi ứng dụng CNTT hàng năm của các cơ quan, đơn vị.

- Điều kiện bảo đảm: sau khi Ủy ban nhân dân thành phố ban hành Quyết định, Công an thành phố sẽ chủ trì, phối hợp với các cơ quan, đơn vị có liên quan tổ chức triển khai thực hiện.

- Thời gian trình ban hành: dự kiến trước ngày 31/12/2025.

Công an thành phố Cần Thơ xin kính trình Ủy ban nhân dân thành phố Cần Thơ xem xét, quyết định./.

(Xin gửi kèm theo: (1) dự thảo Quyết định ban hành kèm Quy chế; (2) Bảng so sánh, thuyết minh nội dung dự thảo Quyết định; (3) 03 phụ lục).

Nơi nhận:
- Như trên;
- Ban Giám đốc CATP;
- Phòng: TM (Đ6), ANM;
- Lưu: VT, ANM (NHKN,02).

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

Đại tá Nguyễn Văn Thắng