ỦY BAN NHÂN DÂN THÀNH PHỐ CẦN THƠ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 210 /KH-UBND	*Cần Thơ, ngày 07 tháng 5 năm 2026*

KẾ HOẠCH

Thực hiện Chương trình số 17-CTr/TU ngày 21/3/2026 của Ban Thường vụ Thành ủy về thực hiện Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị

Thực hiện Chương trình số 17-CTr/TU ngày 21 tháng 3 năm 2026 của Ban Thường vụ Thành ủy về thực hiện Chỉ thị số 57-CT/TW ngày 31 tháng 12 năm 2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị, Ủy ban nhân dân thành phố ban hành Kế hoạch triển khai thực hiện, cụ thể như sau:

I. MỤC ĐÍCH

1. Quán triệt và tổ chức triển khai thực hiện Chỉ thị số 57-CT/TW ngày 31 tháng 12 năm 2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị và Kế hoạch số 04-KH/BCĐTW ngày 05 tháng 01 năm 2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị, tạo sự thống nhất cao trong nhận thức và hành động của toàn Đảng bộ, chính quyền và Nhân dân thành phố.

2. Xác định rõ vai trò, trách nhiệm của người đứng đầu cấp ủy, chính quyền; cụ thể hóa các mục tiêu, nhiệm vụ, giải pháp của Chương trình số 17-CTr/TU thành các nhiệm vụ, giải pháp cụ thể phù hợp với đặc điểm, tình hình thực tế của thành phố, đặc biệt trong bối cảnh triển khai mô hình chính quyền địa phương 02 cấp và đẩy mạnh chuyển đổi số. Nâng cao hiệu quả công tác bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu trên địa bàn, chủ động phòng ngừa, phát hiện và xử lý kịp thời các nguy cơ, sự cố an ninh mạng.

II. YÊU CẦU

1. Các cơ quan, đơn vị quán triệt kế hoạch đến từng cán bộ, đảng viên với phương châm "chủ động phòng ngừa, phát hiện từ sớm, ngăn chặn từ xa"; chuyển dịch tư duy từ "phòng thủ bị động" sang "phòng thủ chủ động", "phòng thủ tích cực". Việc tổ chức thực hiện phải đảm bảo nghiêm túc, thiết thực, hiệu quả, có trọng tâm, trọng điểm; kết hợp chặt chẽ giữa bảo đảm an ninh mạng với phát triển kinh tế - xã hội.

2. Xây dựng không gian mạng trên địa bàn thành phố an toàn, vững mạnh, có năng lực phòng thủ tốt và khả năng chống chịu cao, tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị thành phố.

III. NHIỆM VỤ VÀ GIẢI PHÁP TRỌNG TÂM

1. Nhiệm vụ trọng tâm năm 2026

a) Kiện toàn Tiểu ban An toàn, an ninh mạng thành phố, trong đó Trưởng Tiểu ban là Bí thư Thành ủy;

b) Các cơ quan chủ quản các cơ sở dữ liệu, hệ thống thông tin trên địa bàn thành phố có trách nhiệm: (i) Rà soát, khắc phục tổng thể về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với hệ thống thông tin theo tiêu chuẩn TCVN 14423: 2025 và nguồn nhân lực thuộc phạm vi quản lý; (ii) Triển khai giám sát an ninh mạng tại cơ quan, đơn vị thuộc phạm vi quản lý; (iii) Báo cáo định kỳ và đột xuất kết quả, tiến độ và mức độ tuân thủ về cơ quan có thẩm quyền; kiến nghị biện pháp hoàn thiện thể chế, tiêu chuẩn và phân bổ nguồn lực khi cần; (iv) Xác định trách nhiệm của người đứng đầu về an ninh mạng;

c) Nâng cao năng lực của Đội ứng cứu sự cố an ninh mạng bảo đảm an toàn thông tin mạng thành phố; thiết lập kênh kết nối trao đổi thông tin, dữ liệu phục vụ giám sát, điều phối ứng cứu, khắc phục sự cố an toàn thông tin, an ninh mạng;

d) Tổ chức tập huấn, hướng dẫn triển khai các quy định pháp luật mới, tài liệu về kiểm tra, đánh giá, bảo đảm an ninh mạng, an toàn thông tin cho các cơ sở dữ liệu, hệ thống dùng chung trong hệ thống các cơ quan, đơn vị; định kỳ tổ chức kiểm tra, đánh giá việc thực hiện các quy định đảm bảo an ninh mạng, an toàn thông tin;

đ) Tổ chức thẩm định, phê duyệt cấp độ đối với toàn bộ hệ thống thông tin trọng yếu của thành phố. Đối với hạ tầng và các hệ thống đang xây dựng hoặc sẽ triển khai trong thời gian tới, yêu cầu bắt buộc phải thực hiện phê duyệt cấp độ an toàn thông tin trước khi đưa vào vận hành chính thức. Đối với các hệ thống thông tin và hạ tầng hiện đang sử dụng, cần khẩn trương rà soát, đánh giá và thực hiện phê duyệt cấp độ an toàn thông tin theo đúng quy định;

e) Phối hợp các đơn vị có liên quan rà soát, xem xét ban hành hoặc điều chỉnh quy hoạch để phù hợp hạ tầng công nghệ thông tin tổng thể từ thành phố đến các địa phương theo hướng tập trung, chuẩn hoá trung tâm dữ liệu.

2. Nhiệm vụ đến năm 2030

a) Xây dựng, hoàn thiện thế trận an ninh mạng và hạ tầng kỹ thuật:

- Đầu tư xây dựng Trung tâm An ninh mạng thành phố do Công an thành phố quản lý, vận hành, bảo đảm các tiêu chuẩn kỹ thuật theo hướng dẫn của Bộ Công an. Thực hiện kết nối, chia sẻ dữ liệu giám sát với Trung tâm An ninh mạng quốc gia; bảo đảm 100% hệ thống thông tin của các cơ quan Đảng, Nhà nước trên địa bàn thành phố được bảo vệ theo mô hình 4 lớp và được giám sát an toàn thông tin 24/7;

- Rà soát, sắp xếp lại hạ tầng công nghệ thông tin theo hướng tập trung; kiên quyết thu hồi, loại bỏ các hệ thống thông tin, máy chủ đơn lẻ không đáp ứng tiêu chuẩn an ninh mạng. Đối với hệ thống chính quyền địa phương cấp xã, thực hiện mô hình quản lý tập trung từ thành phố, hạn chế tối đa việc lưu trữ dữ liệu quan trọng tại thiết bị đầu cuối ở cơ sở;

- Thực hiện nghiêm quy định: hồ sơ thiết kế hệ thống thông tin, dự án chuyển đổi số phải có cấu phần an ninh mạng (chiếm tối thiểu 15% tổng mức đầu tư) và phải được thẩm định, phê duyệt về mặt an ninh mạng trước khi đầu tư xây dựng. Hệ thống chưa bảo đảm an toàn tuyệt đối thì không đưa vào vận hành;

- Tổ chức rà soát, kiểm tra, đánh giá định kỳ công tác bảo đảm an ninh thông tin, an ninh mạng; tăng cường phối hợp chặt chẽ, hiệp đồng tác chiến giữa các lực lượng chuyên trách trong bảo vệ an ninh mạng toàn hệ thống chính trị.

b) Nâng cao nhận thức cho toàn hệ thống chính trị và người dân trên địa bàn thành phố:

- Triển khai các chương trình đào tạo, bồi dưỡng, phổ biến kiến thức an ninh mạng trên nền tảng "Bình dân học vụ số";

- Đẩy mạnh truyền thông đại chúng và trên mạng xã hội cho người dân kỹ năng nhận diện, phòng, chống lừa đảo, tiếp nhận và xử lý phản ánh sự cố;

- Nghiên cứu đưa các nội dung kiến thức, kỹ năng cơ bản về an ninh mạng vào chương trình giáo dục phổ thông (từ Trung học cơ sở đến Trung học phổ thông), giáo dục nghề nghiệp và đại học;

- Triển khai, hướng dẫn thực hiện các giải pháp định danh và đánh giá tín nhiệm mạng các tổ chức, cá nhân có ảnh hưởng trên không gian mạng theo quy định từ Trung ương; củng cố lòng tin, trách nhiệm của người dân khi hoạt động, tương tác, làm việc trên không gian mạng;

- Đưa tiêu chí bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu vào đánh giá xếp loại thi đua, khen thưởng của cơ quan, tổ chức, đơn vị.

c) Phát triển nguồn nhân lực và xây dựng "Công dân số":

- Xây dựng cơ chế đặc thù thu hút chuyên gia an ninh mạng chất lượng cao về làm việc tại thành phố; phối hợp với các học viện, trường đại học tổ chức đào tạo, huấn luyện thực chiến định kỳ cho đội ngũ cán bộ chuyên trách;

- Triển khai phong trào "Bình dân học vụ số": tích hợp nội dung an ninh mạng vào chương trình giáo dục ngoại khóa cho học sinh các cấp (từ Trung học cơ sở đến Trung học phổ thông), giáo dục nghề nghiệp và đại học;

- Phát huy vai trò của Tổ Công nghệ số cộng đồng, Đoàn Thanh niên, Hội Phụ nữ trong việc "đi từng ngõ, gõ từng nhà", hướng dẫn người dân kỹ năng bảo vệ dữ liệu cá nhân, sử dụng dịch vụ công an toàn và phòng, chống tin giả;

- Xử lý triệt để tình trạng SIM "rác", tài khoản "ảo", nặc danh; đẩy mạnh xác thực danh tính điện tử (VNeID) nhằm xây dựng môi trường mạng lành mạnh, văn minh.

d) Xây dựng và hoàn thiện thể chế, khung pháp lý:

- Nghiên cứu, phối hợp tham gia góp ý kiến với Bộ, ngành Trung ương trong quá trình xây dựng và hoàn thiện hệ thống văn bản quy phạm pháp luật về an ninh mạng, chuyển đổi số, bảo mật thông tin, an ninh dữ liệu và các văn bản hướng dẫn thi hành, bảo đảm tính thống nhất, đồng bộ và khả thi trong triển khai;

- Xây dựng, điều chỉnh tiêu chuẩn và mô tả vị trí việc làm theo từng lĩnh vực quản lý; bổ sung yêu cầu về kỹ năng số phù hợp với chức năng, nhiệm vụ và công cụ làm việc của từng vị trí, trên cơ sở tham chiếu Khung năng lực số quốc gia và các quy định pháp luật hiện hành;

- Phối hợp với Bộ, ngành Trung ương rà soát và cập nhật tiêu chuẩn và quy chuẩn kỹ thuật đối với sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, đối với các hệ thống thông tin của các cơ quan, đơn vị của thành phố mà có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống Nhân dân;

- Hoàn thiện các cơ chế trao đổi, chia sẻ thông tin giữa các cơ quan, đơn vị của thành phố, nhằm bảo đảm kết nối, liên thông, chia sẻ dữ liệu hiệu quả.

đ) Bảo đảm nguồn lực tài chính và công nghệ:

- Sở Tài chính tham mưu bố trí đầy đủ và kịp thời kinh phí cho công tác an ninh mạng. Trong kế hoạch đầu tư công trung hạn và hằng năm, ưu tiên phân bổ vốn cho các dự án an ninh mạng trọng điểm;

- Ưu tiên sử dụng các sản phẩm, giải pháp an ninh mạng "Make in Vietnam" trong các cơ quan nhà nước; khuyến khích các doanh nghiệp công nghệ số trên địa bàn thành phố tham gia nghiên cứu, phát triển các sản phẩm an ninh mạng.

e) Bảo đảm nguồn nhân lực:

- Xây dựng chương trình đào tạo chuyên sâu, huấn luyện thực tế về công tác an ninh mạng. Tiếp tục hoàn thiện cơ chế, chính sách thu hút, đãi ngộ chuyên gia tham gia phục vụ công tác an ninh mạng quốc gia;

- Triển khai các chương trình đào tạo, bồi dưỡng, nâng cao năng lực chuyên môn, kỹ năng giám sát, điều tra, ứng phó sự cố, bảo vệ dữ liệu, an ninh mạng, an toàn thông tin, bảo mật và tác chiến bảo vệ chủ quyền quốc gia trên không gian mạng; nâng cao năng lực nghiên cứu, phát triển trong an ninh mạng;

- Tăng cường nhân lực bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho Sở, ban, ngành và các địa phương theo quy định.

g) Hợp tác quốc tế trên lĩnh vực an ninh mạng: Triển khai hiệu quả, thực chất Công ước của Liên hợp quốc về phòng, chống tội phạm mạng năm 2025 (Công ước Hà Nội). Tăng cường chia sẻ thông tin, phối hợp điều tra tội phạm mạng xuyên quốc gia; cử cán bộ đi đào tạo, huấn luyện chuyên sâu nâng cao trình độ chuyên môn trong công tác đấu tranh phòng chống tội phạm mạng tại nước ngoài hoặc do các cơ quan, tổ chức quốc tế phối hợp với Bộ, ngành Trung ương và các tỉnh, thành phố tổ chức tại thành phố Cần Thơ.

IV. KINH PHÍ THỰC HIỆN

1. Nguồn kinh phí thực hiện Kế hoạch được bảo đảm từ ngân sách nhà nước theo phân cấp; đồng thời lồng ghép trong các chương trình, đề án, dự án có liên quan và huy động các nguồn vốn hợp pháp khác;

2. Ưu tiên bố trí ngân sách cho các nhiệm vụ cấp bách. Áp dụng linh hoạt các cơ chế tài chính đặc thù đã được cấp có thẩm quyền phê duyệt nhằm đáp ứng yêu cầu tiến độ thực hiện;

3. Việc triển khai các nội dung, nhiệm vụ, giải pháp của Kế hoạch bảo đảm thiết thực, hiệu quả, tránh trùng lặp, lãng phí, tiêu cực.

V. NỘI DUNG NHIỆM VỤ VÀ PHÂN CÔNG TRÁCH NHIỆM

Thực hiện theo Phụ lục đính kèm.

VI. TỔ CHỨC THỰC HIỆN

1. Sở, ban, ngành thành phố, Ủy ban nhân dân xã, phường

a) Người đứng đầu cơ quan, đơn vị và địa phương chịu trách nhiệm lãnh đạo, chỉ đạo, kiểm tra và đôn đốc thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu; chịu trách nhiệm trực tiếp và toàn diện nếu để xảy ra sự cố an ninh mạng nghiêm trọng, đặc biệt là lộ, mất bí mật nhà nước trên không gian mạng do yếu tố chủ quan, thiếu trách nhiệm hoặc không tuân thủ quy định. Đưa kết quả đánh giá chỉ số bảo đảm an ninh mạng của các cơ quan, tổ chức vào tiêu chí đánh giá tín nhiệm, năng lực của cán bộ, nhất là đối với người đứng đầu, để phục vụ công tác xếp loại hằng năm;

b) Chịu trách nhiệm người đứng đầu trước Chủ tịch Ủy ban nhân dân thành phố về kết quả thực hiện các nhiệm vụ được giao tại Kế hoạch này; tổ chức quán triệt, tuyên truyền, phổ biến Chương trình số 17-CTr/TU đến toàn thể cán bộ, đảng viên và Nhân dân. Căn cứ chức năng, nhiệm vụ được phân công, các đơn vị, địa phương xây dựng Kế hoạch chi tiết để lãnh đạo, chỉ đạo và tổ chức thực hiện, đảm bảo hiệu quả, tiến độ, có trọng tâm, trọng điểm nhằm tạo chuyển biến chung tại các cơ quan, đơn vị và địa phương;

c) Về chế độ báo cáo: Định kỳ hằng năm, các cơ quan, đơn vị báo cáo kết quả thực hiện về Ủy ban nhân dân thành phố (qua Công an thành phố) trước ngày 15 tháng 11 hàng năm để tổng hợp, theo dõi.

2. Công an thành phố

a) Tham mưu kiện toàn Tiểu ban An toàn, an ninh mạng thành phố, trong đó Trưởng Tiểu ban là Bí thư Thành ủy;

b) Chịu trách nhiệm về công tác quản lý nhà nước đối với an ninh mạng, bảo mật thông tin, an ninh dữ liệu (trừ quân sự, cơ yếu); quản lý nhà nước đối với sản phẩm mật mã an ninh;

c) Chủ trì hướng dẫn Bộ chỉ số bảo đảm an ninh mạng quốc gia và tổ chức đánh giá, xếp hạng định kỳ hằng năm đối với Sở, ban, ngành, Ủy ban nhân dân xã, phường và các doanh nghiệp viễn thông, công nghệ thông tin trên địa bàn thành phố; ứng dụng sản phẩm mật mã dân sự trong công tác bảo đảm an ninh mạng; chủ trì triển khai các nhiệm vụ về phát triển và ứng dụng sản phẩm mật mã an ninh; vận động, khuyến khích các nguồn lực xã hội tham gia bảo đảm an ninh mạng trên địa bàn thành phố;

d) Chủ trì, phối hợp với các đơn vị liên quan đẩy mạnh kết nối, sử dụng dữ liệu từ Cơ sở dữ liệu quốc gia về dân cư để thống nhất định danh không gian mạng toàn diện; tập trung chỉ đạo xử lý dứt điểm tình trạng SIM "rác", tài khoản "ảo"; thiết lập trật tự, kỷ cương trong quản lý người dùng mạng xã hội; bảo đảm công tác bảo vệ an ninh mạng, bảo vệ dữ liệu cá nhân và bảo vệ trẻ em trên không gian mạng trên địa bàn thành phố;

đ) Chủ trì, phối hợp với các đơn vị liên quan trong thực hiện công tác tuyên truyền, phổ biến giáo dục pháp luật về an ninh mạng, bảo mật thông tin, an ninh dữ liệu; giáo dục kỹ năng bảo vệ dữ liệu cá nhân, phòng, chống tội phạm lừa đảo, chiếm đoạt tài sản trên không gian mạng;

e) Phối hợp với Văn phòng Ủy ban nhân dân thành phố và các đơn vị liên quan tham mưu theo dõi, đôn đốc, kiểm tra, tổng hợp, báo cáo kết quả việc thực hiện Kế hoạch này theo quy định.

3. Sở Khoa học và Công nghệ

a) Chủ trì, phối hợp với Sở, ban, ngành thành phố và Ủy ban nhân dân xã, phường triển khai các chương trình đào tạo, bồi dưỡng, phổ biến kiến thức an ninh mạng trên nền tảng "Bình dân học vụ số";

b) Chủ trì, phối hợp với các cơ quan, đơn vị liên quan khuyến khích các doanh nghiệp công nghệ số trên địa bàn thành phố tham gia nghiên cứu, phát triển các sản phẩm an ninh mạng; thúc đẩy ưu tiên sử dụng các sản phẩm, giải pháp an ninh mạng "Make in Vietnam" trong các cơ quan nhà nước;

c) Phối hợp với Công an thành phố tổ chức rà soát, đánh giá tổng thể và khắc phục các lỗ hổng bảo mật về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với hệ thống thông tin theo tiêu chuẩn TCVN 14423:2025 và nguồn nhân lực thuộc phạm vi quản lý.

d) Phối hợp với Công an thành phố và các đơn vị có liên quan triển khai giám sát an ninh mạng tại cơ quan, đơn vị thuộc phạm vi quản lý; phối hợp triển khai mô hình bảo đảm an toàn thông tin "4 lớp" cho các hệ thống thông tin trên địa bàn thành phố gồm: (i) Lực lượng tại chỗ chịu trách nhiệm vận hành, giám sát và ứng cứu ban đầu khi sự cố xảy ra; (ii) Hệ thống hoặc dịch vụ giám sát 24/7, giúp phát hiện sớm các nguy cơ; (iii) Đơn vị độc lập thực hiện kiểm tra, đánh giá định kỳ để đảm bảo khách quan và minh bạch; (iv) Kết nối, chia sẻ thông tin với hệ thống giám sát an ninh mạng quốc gia, bảo đảm sự phối hợp liên thông trên phạm vi toàn quốc (trừ các hệ thống thông tin quân sự, quốc phòng, cơ yếu).

4. Sở Giáo dục và Đào tạo

a) Tích hợp nội dung an ninh mạng vào chương trình giáo dục ngoại khóa cho học sinh các cấp (từ Trung học cơ sở đến Trung học phổ thông), giáo dục nghề nghiệp;

b) Chủ trì, phối hợp với Công an thành phố và các đơn vị liên quan xây dựng và triển khai các chương trình đào tạo, tập huấn, bồi dưỡng kiến thức, kỹ năng sư phạm, tuyên truyền bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

5. Các cơ sở giáo dục đại học trên địa bàn

a) Tích hợp các nội dung kiến thức, kỹ năng cơ bản về an ninh mạng vào chương trình giáo dục (chính khóa hoặc ngoại khóa) cho học viên, sinh viên của cơ sở mình; tích cực hưởng ứng triển khai phong trào "Bình dân học vụ số";

b) Chủ trì, phối hợp với Công an thành phố xây dựng và triển khai các chương trình đào tạo, tập huấn, bồi dưỡng kiến thức, kỹ năng sư phạm, tuyên truyền bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho cán bộ, giảng viên, sinh viên; đồng thời phối hợp tổ chức đào tạo, huấn luyện thực chiến định kỳ cho đội ngũ cán bộ chuyên trách của thành phố; cử chuyên gia có kinh nghiệm tham gia Đội ứng cứu sự cố an toàn thông tin mạng thành phố.

6. Sở Tài chính

a) Chủ trì, phối hợp với các đơn vị liên quan đảm bảo kinh phí đầu tư từ ngân sách nhà nước cho hoạt động an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho các cơ quan, đơn vị và địa phương. Hướng dẫn các cơ quan, đơn vị và địa phương bảo đảm kinh phí đầu tư từ ngân sách cho các hoạt động an ninh mạng, bảo mật thông tin, an ninh dữ liệu;

b) Chủ trì, phối hợp với các đơn vị liên quan hướng dẫn các quy định về tài chính, tài sản công, ngân sách, đấu thầu có liên quan để tạo thuận lợi trong quá trình triển khai thực hiện, đáp ứng yêu cầu nhiệm vụ và đặc thù vòng đời của sản phẩm an ninh mạng thường ngắn hơn quy định về khấu hao tài sản công.

7. Sở Văn hóa, Thể thao và Du lịch

Chủ trì, phối hợp với các đơn vị liên quan đẩy mạnh công tác tuyên truyền, phổ biến giáo dục pháp luật về an ninh mạng, bảo mật thông tin, an ninh dữ liệu trên các phương tiện thông tin đại chúng, hệ thống truyền thông tại cơ sở và hệ thống cổ động trực quan; lồng ghép truyền thông, giáo dục cho người dân kỹ năng bảo vệ dữ liệu cá nhân, nhận diện và phòng, chống tội phạm lừa đảo, chiếm đoạt tài sản trên không gian mạng thông qua các hoạt động văn hóa, thể thao và du lịch.

8. Các doanh nghiệp viễn thông, công nghệ thông tin trên địa bàn thành phố

a) Các doanh nghiệp tham gia chủ trì, đồng hành trong hoạt động chuyển đổi số tại các cơ quan, đơn vị và địa phương có trách nhiệm phối hợp chặt chẽ với cơ quan, đơn vị chủ quản trong việc thực hiện đầy đủ các quy định của pháp luật về bảo đảm an ninh mạng, an toàn thông tin và bảo vệ dữ liệu trong quá trình thiết kế, triển khai, vận hành hệ thống thông tin, nền tảng số, dịch vụ số; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng, bảo vệ dữ liệu cá nhân; chịu trách nhiệm trước cơ quan chủ quản, cơ quan có thẩm quyền nếu để xảy ra sự cố, rò rỉ, mất an toàn thông tin do lỗi chủ quan hoặc vi phạm quy trình;

b) Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet trên địa bàn thành phố phát huy vai trò là tuyến đầu phòng thủ và có trách nhiệm tuân thủ quy định trong công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

Trên đây là Kế hoạch thực hiện Chương trình số 17-CTr/TU ngày 21 tháng 3 năm 2026 của Ban Thường vụ Thành ủy về thực hiện Chỉ thị số 57-CT/TW ngày 31 tháng 12 năm 2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị. Trong quá trình triển khai thực hiện, nếu phát sinh khó khăn, vướng mắc các cơ quan, đơn vị và địa phương kịp thời phản ánh về Công an thành phố (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để tổng hợp, báo cáo Ủy ban nhân dân thành phố xem xét, giải quyết./.

Nơi nhận:
- Văn phòng Chính phủ;
- Bộ Công an;
- Thường trực: TU, HĐND TP;
- CT và các PCT UBND TP;
- UBMTTQVN và các đoàn thể TP;
- Sở, ban, ngành TP;
- UBND xã, phường;
- Báo và PTTH CT;
- Các cơ sở giáo dục ĐH trên địa bàn;
- Các DN Viễn thông, CNTT trên địa bàn;
- VP UBND TP (2A, 3C);
- Cổng TTĐT TP;
- Lưu: VT, VHQ.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

ỦY BAN NHÂN DÂN THÀNH PHỐ CẦN THƠ

Trương Cảnh Tuyên