ỦY BAN NHÂN DÂN THÀNH PHỐ HUẾ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 226 /KH-UBND	*Huế, ngày 17 tháng 4 năm 2026*

KẾ HOẠCH

Triển khai Chương trình hành động thực hiện Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư Trung ương Đảng 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 hành động số 27-CTr/TU, ngày 10/3/2026 của Thành ủy và Kế hoạch số 26-KH/ĐU, ngày 16/3/2026 của Đảng ủy UBND thành phố về thực hiện Chỉ thị số 57-CT/TW, ngày 31/12/2025 của Ban Bí thư Trung ương Đảng về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị (gọi tắt là Chỉ thị số 57-CT/TW, Chương trình số 27-CTr/TU), UBND thành phố ban hành kế hoạch thực hiện như sau:

I. MỤC ĐÍCH, YÊU CẦU

- Thủ trưởng các cơ quan, đơn vị, địa phương tăng cường lãnh đạo, chỉ đạo toàn diện các mặt công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trên địa bàn thành phố; thường xuyên kiểm tra, giám sát việc thực hiện các quy định bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

- Không để bị động, bất ngờ trong mọi tình huống; mọi nguy cơ, thách thức về an ninh mạng, bảo mật thông tin, an ninh dữ liệu phải được nhận diện và xử lý từ sớm; gắn chặt các yếu tố bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu ngay từ khi thiết kế, xây dựng hệ thống, trong quá trình vận hành, kết nối.

- Phát huy sức mạnh tổng hợp của cả hệ thống chính trị và toàn dân để thực hiện hiệu quả công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu với nòng cốt là lực lượng chuyên trách công tác bảo đảm an ninh mạng, an toàn thông tin.

II. NHIỆM VỤ, GIẢI PHÁP TRỌNG TÂM

1. Nâng cao nhận thức, trách nhiệm của cán bộ, đảng viên, công chức, viên chức, người lao động, học sinh, sinh viên; quyết liệt trong lãnh đạo, chỉ đạo nhằm bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu

- Tăng cường công tác tuyên truyền, quán triệt Chỉ thị số 57-CT/TW, Chương trình 27-CTr/TU đến toàn thể cán bộ, đảng viên, công chức, viên chức, người lao động, học sinh, sinh viên, góp phần nâng cao nhận thức, kỹ năng, trách nhiệm, tạo sự đồng thuận cao trong thực hiện hiệu quả công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu, bảo vệ bí mật nhà nước tại cơ quan, đơn vị, doanh nghiệp.

- Thủ trưởng các cơ quan, đơn vị, địa phương xác định nhiệm vụ về bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu, bảo vệ bí mật nhà nước là nhiệm vụ quan trọng, thường xuyên trong công tác lãnh đạo, chỉ đạo và quản lý, điều hành; quan tâm công tác xây dựng cán bộ chuyên trách bảo đảm an ninh mạng, công nghệ thông tin; bảo đảm điều kiện cơ sở vật chất phục vụ công tác đảm bảo an ninh mạng, bảo mật thông tin, an ninh dữ liệu; chịu trách nhiệm trực tiếp, toàn diện về công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước tại địa phương, đơn vị mình quản lý. Kết quả công tác này là một trong những tiêu chí quan trọng để đánh giá, xếp loại tổ chức, cán bộ, đảng viên, công chức, viên chức và người lao động hằng năm.

- Nghiên cứu, đưa nội dung đào tạo về kiến thức, kỹ năng cơ bản về an ninh mạng, an toàn thông tin vào chương trình giáo dục phổ thông và các cơ sở giáo dục đào tạo nghề nghiệp, các trường cao đẳng, đại học trên địa bàn khi có hướng dẫn của cấp trên. Tăng cường phối hợp với các cơ quan, đơn vị đẩy mạnh công tác tuyên truyền, phổ biến, đào tạo kiến thức an ninh mạng, an toàn thông tin, kỹ năng bảo vệ dữ liệu cá nhân, phòng, chống tội phạm lừa đảo trực tuyến trên nền tảng "Bình dân học vụ số" để xây dựng "thế hệ công dân số" văn minh, tuân thủ pháp luật.

- Triển khai đánh giá tín nhiệm mạng; phát động phong trào toàn dân bảo vệ an ninh mạng; phát huy trách nhiệm xã hội của cơ quan báo chí và người có uy tín trong việc định hướng dư luận, lan toả thông tin tích cực và đấu tranh với các thông tin xấu độc.

2. Khẩn trương hoàn thiện, triển khai hiệu quả các thể chế, chính sách và nâng cao hiệu lực, hiệu quả quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu

- Chủ động rà soát, đề xuất sửa đổi, bổ sung, hoàn thiện hành lang pháp lý cho an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

- Triển khai, áp dụng các thể chế, chính sách pháp luật về công tác bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn, gồm: áp dụng các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật về bảo đảm an ninh mạng; triển khai Khung quản lý rủi ro an ninh mạng và chỉ số đánh giá năng lực bảo đảm an ninh mạng của các cơ quan, đơn vị, địa phương.

- Quy hoạch và phát triển hạ tầng số, hạ tầng dữ liệu của thành phố bảo đảm hiện đại, đồng bộ, an toàn. Thực hiện nghiêm quy định pháp luật yêu cầu hồ sơ thiết kế hệ thống thông tin, dự án chuyển đổi số phải có cấu phần an ninh mạng được thẩm định, phê duyệt trước khi đầu tư xây dựng.

- Nghiên cứu tham mưu xây dựng cơ chế, chính sách đặc thù trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo để phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng, an ninh dữ liệu; xây dựng cơ chế, chính sách hỗ trợ, thu hút doanh nghiệp công nghệ, cộng đồng khởi nghiệp sáng tạo tham gia phát triển cộng

đồng doanh nghiệp an ninh mạng vững mạnh ở thành phố Huế, thu hút, đãi ngộ chuyên gia giỏi, nhân tài tham gia nghiên cứu khoa học, phát triển công nghệ, đổi mới sáng tạo phục vụ công tác an ninh mạng trên địa bàn thành phố.

- Triển khai, thực hiện nghiêm túc cơ chế trao đổi, chia sẻ thông tin và quy trình phối hợp ứng cứu sự cố theo Phương án xử lý sự cố an ninh mạng đã được UBND thành phố ban hành.

- Phối hợp các doanh nghiệp viễn thông, Internet, tài chính, ngân hàng trong việc bảo đảm an ninh hệ thống; phối hợp thiết lập cơ chế cung cấp dữ liệu, chứng cứ điện tử nhanh chóng, kịp thời, bảo đảm "đúng, đủ, sạch, sống" để phục vụ công tác điều tra, xử lý tội phạm và bảo vệ chủ quyền quốc gia; đơn giản hoá thủ tục hành chính trong các tình huống khẩn cấp về an ninh mạng.

3. Tập trung đầu tư, hiện đại hoá hạ tầng, công nghệ và các giải pháp kỹ thuật bảo đảm an ninh mạng

- Quan tâm bố trí nguồn lực đầu tư, nâng cấp, hoàn thiện hạ tầng công nghệ thông tin phục vụ cho công tác chuyên môn gắn với triển khai các giải pháp kỹ thuật nhằm bảo đảm an toàn thông tin, an ninh kết nối. Thực hiện nghiêm quy định ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng "Make in Vietnam" trong các dự án đầu tư công. Thực hiện đúng yêu cầu bảo đảm tỉ lệ kinh phí chi cho an ninh mạng, bảo mật thông tin đạt tối thiểu 15% tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số; đầu tư có trọng tâm, trọng điểm, tránh dàn trải, lãng phí.

- Tập trung hoàn thiện, từng bước nâng cao năng lực Trung tâm giám sát an ninh mạng, an toàn thông tin tập trung (SOC) thành phố Huế, hình thành Trung tâm An ninh mạng đáp ứng công tác bảo đảm an ninh mạng, an toàn dữ liệu trên địa bàn thành phố Huế; có khả năng tích hợp, kết nối với các sản phẩm an ninh mạng phù hợp, đáp ứng tiêu chuẩn, quy chuẩn về an ninh mạng; mở rộng kết nối giám sát an ninh mạng đến các hệ thống thông tin, hệ thống dùng chung của toàn hệ thống chính trị và các cơ quan, đơn vị, doanh nghiệp trọng yếu.

- Triển khai, áp dụng các hệ thống tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an ninh mạng; áp dụng giải pháp kỹ thuật bảo đảm tuyệt đối an toàn cho các hệ thống thông tin trọng yếu. Tổ chức rà soát, kiểm tra, đánh giá định kỳ công tác bảo đảm an ninh thông tin, an ninh mạng.

4. Xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng; phát triển tiềm lực, công nghệ và nguồn nhân lực

- Các cơ quan, đơn vị, địa phương xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng; phát huy vai trò của cả hệ thống chính trị trong công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu. Phát huy vai trò, trách nhiệm của các cơ quan, tổ chức, doanh nghiệp

và cán bộ, đảng viên, công chức, người lao động, học sinh, sinh viên trong việc tham gia bảo vệ an ninh mạng; xây dựng môi trường không gian mạng an toàn, lành mạnh.

- Ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng "Make in Vietnam" trong công tác bảo mật thông tin, an ninh dữ liệu.

- Các đơn vị giáo dục và đào tạo, khoa học và công nghệ... có kế hoạch đào tạo chuyên sâu về bảo đảm an ninh mạng, phát triển đội ngũ giảng viên, các nhà khoa học đủ năng lực, trình độ đáp ứng việc giảng dạy các chuyên ngành liên quan tại các trường đại học; đẩy mạnh hợp tác với các trường đại học uy tín trong và ngoài nước. Quan tâm phát triển nguồn nhân lực công nghệ thông tin và an toàn thông tin trong các cơ quan nhà nước; tăng cường đào tạo, bồi dưỡng, nâng cao trình độ chuyên môn, kỹ năng cho đội ngũ cán bộ, công chức, viên chức làm công tác công nghệ thông tin và an ninh mạng.

- Khuyến khích nghiên cứu, ứng dụng, chuyển giao các thành tựu khoa học, công nghệ mới trong lĩnh vực công nghệ thông tin, an ninh mạng; từng bước nâng cao tiềm lực công nghệ phục vụ công tác bảo đảm an ninh mạng của thành phố.

- Tăng cường phối hợp với các cơ quan chức năng tổ chức tập huấn kỹ năng, nghiệp vụ về công tác bảo đảm an ninh mạng cho cán bộ chuyên trách công nghệ thông tin tại các cơ quan, đơn vị, địa phương.

5. Tăng cường hợp tác quốc tế trên lĩnh vực an ninh mạng

- Tăng cường hợp tác, trao đổi, nghiên cứu khoa học, phát triển công nghệ, chuyển đổi số với các chuyên gia, tổ chức, doanh nghiệp, địa phương trong nước và quốc tế trong lĩnh vực bảo đảm an ninh mạng, khoa học công nghệ, nghiên cứu, phát triển, ứng dụng thuật toán mật mã kháng lượng tử để bảo vệ bí mật nhà nước.

- Nghiên cứu đề xuất các chính sách khuyến khích mua, chuyển giao công nghệ tiên tiến phù hợp với điều kiện của cơ quan, đơn vị. Khuyến khích các chương trình trao đổi khoa học, hỗ trợ chuyển giao công nghệ và phát triển nguồn nhân lực bảo đảm an ninh mạng.

- Tổ chức các hội nghị, hội thảo, tiếp thu kinh nghiệm, công nghệ và chuẩn mực quốc tế về an ninh mạng.

III. TỔ CHỨC THỰC HIỆN

1. Các cơ quan, đơn vị, địa phương

- Tập trung chỉ đạo tổ chức quán triệt, tuyên truyền sâu rộng nội dung Chỉ thị số 57-CT/TW, Chương trình hành động số 27-CTr/TU và Kế hoạch này đến cán bộ, đảng viên, công chức, viên chức, người lao động, học sinh, sinh viên trong cơ quan, đơn vị, địa phương.

- Căn cứ chức năng, nhiệm vụ và điều kiện thực tiễn của cơ quan, đơn vị, địa phương xây dựng kế hoạch thực hiện gắn với việc đẩy mạnh chuyển đổi số,

ứng dụng khoa học, công nghệ vào công tác chuyên môn.

- 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 do yếu tố chủ quan, thiếu trách nhiệm hoặc không tuân thủ quy định.

- Đối với hạ tầng và các hệ thống thông tin 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, khẩn trương rà soát, đánh giá và thực hiện phê duyệt cấp độ an toàn thông tin theo đúng quy định.

2. Công an thành phố:

- Chủ trì quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với các hệ thống thông tin, cơ sở dữ liệu của các hệ thống thông tin trên địa bàn thành phố và quản lý hoạt động cung cấp sản phẩm, dịch vụ an ninh mạng đối với các hệ thống này *(trừ hệ thống thông tin, cơ sở dữ liệu quân sự và cơ yếu thuộc phạm vi Bộ Quốc phòng, Ban Cơ yếu chính phủ quản lý).*

- Tham mưu triển khai Bộ chỉ số bảo đảm an ninh mạng quốc gia và tổ chức đánh giá, xếp hạng định kỳ hằng năm đối với các sở, ban, ngành, địa phương khi có hướng dẫn của cấp trên.

- Nghiên cứu ứng dụng sản phẩm mật mã dân sự vào công tác bảo đảm an ninh mạng quốc gia theo quy định; chủ trì triển khai các nhiệm vụ về phát triển và ứng dụng sản phẩm mật mã an ninh; tham mưu huy động các nguồn lực xã hội tham gia bảo vệ an ninh mạng quốc gia.

- Tham mưu việc 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; tham mưu phối hợp xử lý dứt điểm tình trạng SIM "rác", tài khoản "ảo" và thiết lập trật tự, kỷ cương trong quản lý người dùng mạng xã hội; bảo đảm các yêu cầu về bảo vệ an ninh mạng quốc gia, bảo vệ dữ liệu cá nhân và bảo vệ trẻ em trên không gian mạng.

3. Sở Khoa học và Công nghệ: Phối hợp các đơn vị liên quan triển khai hợp nhất hạ tầng số theo kế hoạch đã được ban hành, đảm bảo trung tâm dữ liệu dùng chung của thành phố đạt chuẩn, đủ điều kiện để triển khai đầy đủ các biện pháp bảo vệ an ninh mạng theo quy định.

4. Bộ Chỉ huy Quân sự thành phố: Chịu trách nhiệm về công tác bảo đảm an ninh mạng, mật mã, bảo mật thông tin trong lĩnh vực quân sự, cơ yếu thuộc phạm vi quản lý của Bộ Quốc phòng.

5. Sở Tài chính: Tham mưu UBND thành phố xem xét, bố trí, bảo đảm kinh phí đầu tư từ nguồn ngân sách và từ các nguồn kinh phí hợp pháp khác cho các hoạt động an ninh mạng, bảo mật thông tin và an ninh dữ liệu tại địa phương theo đúng quy định.

6. Sở Ngoại vụ: Phối hợp chặt chẽ với Công an thành phố, Văn phòng

UBND thành phố, Sở Khoa học và Công nghệ và các đơn vị có liên quan trong việc hợp tác nghiên cứu khoa học, phát triển công nghệ, chuyển đổi số với các chuyên gia, tổ chức, doanh nghiệp quốc tế trong lĩnh vực bảo đảm an ninh mạng; tổ chức các chương trình trao đổi khoa học, hỗ trợ chuyển giao công nghệ và phát triển nguồn nhân lực bảo đảm an ninh mạng.

7. Đại học Huế, Trường Cao đẳng Huế, Sở Giáo dục và Đào tạo thành phố, các đơn vị trường học

- Phối hợp 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 về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trên nền tảng "Bình dân học vụ số".

- Tăng cường phối hợp với các cơ quan, đơn vị tổ chức tuyên truyền, tập huấn kỹ năng bảo vệ dữ liệu cá nhân, an toàn thông tin, phòng, chống tội phạm lừa đảo trên mạng... cho cán bộ, đảng viên, công chức, viên chức, người lao động, học sinh, sinh viên trên địa bàn.

8. Các doanh nghiệp cung cấp dịch vụ trên không gian mạng (bao gồm cả dịch vụ xuyên biên giới), các doanh nghiệp tham gia chủ trì, đồng hành trong hoạt động chuyển đổi số tại các cơ quan, đơn vị, địa phương: 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.

9. Giao Công an thành phố phối hợp các cơ quan, đơn vị theo dõi, đôn đốc việc thực hiện kế hoạch này; định kỳ hằng quý (trước ngày 15 của tháng cuối quý), hằng năm (trước ngày 15 tháng 12) tham mưu UBND thành phố báo cáo Đảng ủy UBND thành phố kết quả thực hiện theo quy định./.

Nơi nhận:
- Thường trực Thành ủy (b/c);
- Thường trực HĐND thành phố (b/c);
- Đảng ủy UBND thành phố (b/c);
- CT và các PCT UBND thành phố;
- Các sở, ban, ngành thành phố;
- Các cơ quan Trung ương trên địa bàn thành phố;
- UBND các xã, phường;
- Lưu: VT, TĐKT.

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

Trần Hữu Thùy Giang