

KẾ HOẠCH

**Triển khai thực hiện Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026
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 tại Đảng bộ Ủy ban nhân dân Thành phố**

Căn cứ Kế hoạch số 34-KH/BCĐTP ngày 05 tháng 5 năm 2026 của Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số Thành phố Hồ Chí Minh về triển khai thực hiện Kế hoạch số 04-KH/BCĐTW, ngày 05/01/2026 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 trên địa bàn Thành phố.

Đảng ủy Ủy ban nhân dân Thành phố ban hành Kế hoạch Triển khai thực hiện Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 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 tại Đảng bộ Ủy ban nhân dân Thành phố như sau:

I. MỤC TIÊU VÀ YÊU CẦU

1. Mục tiêu

a) Trong năm 2026

- **Về công tác lãnh đạo, chỉ đạo:** Tạo chuyển biến mạnh mẽ về nhận thức và hành động trong toàn Đảng bộ.

- **Về thể chế:** phối hợp để triển khai các quy định, hướng dẫn về khuyến khích đổi mới sáng tạo, tạo điều kiện cho doanh nghiệp mới tham gia thị trường, tiếp tục được hoàn thiện gỡ bỏ các rào cản thủ tục.

- **Về hạ tầng:** (1) Các hệ thống thông tin của cơ quan Đảng, Nhà nước và các tổ chức chính trị - xã hội được rà soát, khắc phục các lỗ hổng, điểm yếu an ninh mạng; (2) Các hệ thống thông tin quan trọng thuộc danh mục được ưu tiên bảo vệ của hệ thống chính trị từ cấp độ 3 trở lên được kết nối, chia sẻ thông tin, dữ liệu giám sát an ninh mạng 24/7 với Trung tâm An ninh mạng quốc gia (Bộ Công an); (3) Phối hợp xây dựng và ban hành các tiêu chuẩn, quy chuẩn kỹ thuật cho sản phẩm, dịch vụ an ninh mạng.

- **Nhân lực:** Nâng cao nhận thức của cán bộ, đảng viên và người dân về bảo mật thông tin, an ninh mạng và an ninh dữ liệu; Đào tạo, bồi dưỡng đội ngũ chuyên gia an ninh mạng chất lượng cao.

- **Quản trị:** Tăng cường kỷ luật, kỷ cương trong quản lý nhà nước về an ninh mạng; thực hiện quản trị an ninh mạng dựa trên đánh giá rủi ro, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật.

- **Công nghệ:** Thúc đẩy ứng dụng các công nghệ tiên tiến như trí tuệ nhân tạo, phân tích dữ liệu lớn, giám sát thông minh để phát hiện sớm và xử lý kịp thời các mối đe dọa mạng. Chuyển đổi sang mô hình phòng thủ chủ động, các giải pháp mã hóa hiện đại phục vụ bảo vệ dữ liệu quan trọng, dữ liệu bí mật và giao dịch của Nhà nước. Khuyến khích nghiên cứu, phát triển và làm chủ các công nghệ an ninh mạng thế hệ mới, tăng cường năng lực tự chủ công nghệ, hình thành hệ sinh thái công nghiệp an ninh mạng quốc gia vững mạnh.

b) Đến năm 2030

- **Thể chế:** Hoàn thiện cơ chế pháp lý để khuyến khích đổi mới sáng tạo, tạo điều kiện cho doanh nghiệp mới tham gia thị trường, sản phẩm, giải pháp an ninh mạng chất lượng có cơ hội phát triển. Các quy định của pháp luật đủ sức răn đe và phản ứng nhanh với các hành vi vi phạm pháp luật trên không gian mạng.

- **Hạ tầng:** Đưa vào vận hành hiệu quả kiến trúc bảo vệ an ninh mạng quốc gia đa lớp hiện đại, đồng bộ, hiệu quả bảo đảm chủ quyền quốc gia trên không gian mạng, bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

- **Nhân lực:** Đào tạo và xây dựng được đội ngũ chuyên gia an ninh mạng trình độ cao, đáp ứng nhu cầu trong nước và quốc tế.

- **Quản trị:** Triển khai và áp dụng hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia.

- **Công nghệ:** Tỉ trọng sản phẩm, dịch vụ an ninh mạng “Make in Vietnam” chiếm 50% thị trường trong nước và bắt đầu hình thành năng lực xuất khẩu đạt chuẩn quốc tế. Tự chủ nghiên cứu, sản xuất và làm chủ công nghệ lõi đối với các sản phẩm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

c) Tầm nhìn chiến lược đến năm 2045

Xây dựng nền an ninh mạng quốc gia bền vững, tự chủ, có năng lực cạnh tranh toàn cầu. Hình thành đội ngũ chuyên gia đầu ngành, nhà khoa học công nghệ số trình độ quốc tế; làm chủ các công nghệ cốt lõi, giảm phụ thuộc nhập khẩu. Phát triển hạ tầng an ninh mạng và hạ tầng số hiện đại; xây dựng các trung tâm đổi mới

sáng tạo, khu công nghiệp công nghệ cao; doanh nghiệp trong nước trở thành trụ cột của ngành công nghiệp an ninh mạng Việt Nam.

2. Yêu cầu

- Kế hoạch phải được quán triệt và triển khai thống nhất trong toàn Đảng bộ, tránh dàn trải, cục bộ, thiếu tập trung.
- Nhiệm vụ phải được tổ chức thực hiện với quyết tâm cao, có sản phẩm cụ thể, đo lường được, bảo đảm tiến độ và hiệu quả thực chất.
- Phát huy tối đa tiềm năng, trí tuệ Việt Nam, gắn với tiếp thu, làm chủ và ứng dụng hiệu quả các thành tựu công nghệ, kỹ thuật tiên tiến của thế giới.
- Gắn trách nhiệm người đứng đầu với kết quả bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; coi đây là tiêu chí quan trọng trong đánh giá, quy hoạch, bổ nhiệm cán bộ lãnh đạo, quản lý các cấp.

II. NHIỆM VỤ TRỌNG TÂM NĂM 2026

1. Các cơ quan chủ quản các cơ sở dữ liệu, hệ thống thông tin 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.

3. Xây dựng, đưa vào vận hành Trung tâm An ninh mạng Thành phố¹; mở rộng kết nối, chia sẻ dữ liệu giám sát, cảnh báo an ninh mạng đối với hệ thống thông tin quan trọng của hệ thống chính trị từ cấp độ 3 trở lên; 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.

4. Tham gia tích cực vào hoạt động của liên minh ứng phó sự cố an ninh mạng quốc gia nhằm bảo vệ an ninh mạng vòng ngoài cho các hệ thống thông tin, tài nguyên trọng yếu trên internet của các sở, ban, ngành, địa phương, cơ quan, doanh nghiệp trên địa bàn Thành phố.

5. Ban hành các quy định, tài liệu hướng dẫn 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

¹ Kế hoạch số 133/KH-UBND ngày 20/10/2025 của Ủy ban nhân dân Thành phố về đảm bảo an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn Thành phố Hồ Chí Minh trong năm 2025.

hệ thống chính trị; định kỳ tổ chức kiểm tra, đánh giá việc thực hiện các quy định đảm bảo an ninh mạng, an toàn thông tin theo quy định.

6. Nghiên cứu ban hành cơ chế ưu đãi đặc biệt và chính sách ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng, bảo mật thông tin và an ninh dữ liệu “Make in Vietnam”; từng bước hình thành hệ sinh thái an ninh mạng quốc gia vững mạnh, nâng cao năng lực cạnh tranh đáp ứng nhu cầu xuất khẩu, tham gia sâu vào chuỗi giá trị toàn cầu.

7. Rà soát, trình cấp có thẩm quyền xem xét ban hành hoặc điều chỉnh quy hoạch hạ tầng công nghệ thông tin tổng thể theo hướng tập trung, chuẩn hóa Trung tâm dữ liệu. Đầu tư, nâng cấp hạ tầng công nghệ thông tin đáp ứng yêu cầu và tuân thủ quy hoạch đã được ban hành.

III. NHIỆM VỤ ĐẾN NĂM 2030

1. Nâng cao nhận thức cho toàn hệ thống chính trị và người dân

a) 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) Đổi mới mạnh mẽ nội dung, hình thức truyền thông đại chúng và trên không gian mạng; phát động phong trào thi đua “Dân vận khéo trên không gian mạng” để phổ cập kỹ năng nhận diện, phòng chống lừa đảo trực tuyến.

c) 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.

d) Triển khai các giải pháp định danh và đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng; củng cố lòng tin, trách nhiệm của người dân khi hoạt động, tương tác, làm việc trên không gian mạng.

đ) 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.

2. Xây dựng và hoàn thiện thể chế, khung pháp lý

a) Tiếp tục rà soát, sửa đổi, bổ sung, hoàn thiện hành lang pháp lý cho an ninh mạng, bảo mật thông tin, an ninh dữ liệu, bảo đảm thể chế đi trước một bước.

b) Hoàn thiện, áp dụng các tiêu chuẩn quốc gia và quy chuẩn kỹ thuật đối với các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, áp dụng trước hết đối với hạ tầng thông tin, hệ thống thông tin của các cơ quan trong hệ thống chính trị mà có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống nhân dân.

c) Xây dựng, triển khai Khung quản trị rủi ro an ninh mạng quốc gia và chỉ số đánh giá năng lực bảo đảm an ninh mạng.

d) Hoàn thiện các cơ chế trao đổi, chia sẻ thông tin trong nước và quốc tế về an ninh mạng.

3. Phát triển hạ tầng an ninh mạng hiện đại, đồng bộ, đáp ứng yêu cầu bảo vệ chủ quyền quốc gia trên không gian mạng

a) Triển khai kiến trúc bảo vệ an ninh mạng quốc gia đa lớp hỗ trợ bảo vệ cho toàn bộ hạ tầng mạng Internet và các hệ thống thông tin của các sở, ban, ngành, địa phương, tổ chức, doanh nghiệp.

b) Quy hoạch và triển khai đồng bộ các nhóm giải pháp: (i) Bảo vệ hạ tầng mạng; (ii) Bảo vệ thiết bị đầu cuối; (iii) Bảo vệ ứng dụng, dịch vụ; (iv) Bảo vệ dữ liệu; (v) Bảo vệ người dùng.

c) Bảo vệ tuyệt đối an toàn các hệ thống thông tin quan trọng, các cơ sở dữ liệu về dân cư, đất đai, tài chính, y tế, giáo dục, bảo hiểm, tư pháp,... Thiết lập cơ chế thống nhất về tiêu chuẩn, quy chuẩn bảo mật; bảo đảm an ninh mạng “ngay từ thiết kế” đối với các trung tâm dữ liệu quan trọng, các hệ thống số, nền tảng số và ứng dụng mới; khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin. Kết nối, chia sẻ dữ liệu liên thông giữa các sở, ban, ngành, địa phương trên nguyên tắc bảo mật, an toàn, đúng pháp luật, khắc phục tình trạng cát cứ, phân mảnh dữ liệu.

4. Phát triển công nghiệp an ninh mạng tự chủ và thị trường an ninh mạng cạnh tranh, minh bạch

a) Nghiên cứu xây dựng cơ chế đầu tư cho phát triển hệ sinh thái an ninh mạng, đặc biệt là hệ sinh thái “Make in Vietnam”; ưu tiên làm chủ và sản xuất nội địa các sản phẩm an ninh mạng cốt lõi, nền tảng.

b) Xây dựng thị trường cạnh tranh lành mạnh, minh bạch. Hình thành các trung tâm nghiên cứu, vườn ươm hỗ trợ khởi nghiệp và không gian đổi mới sáng tạo để hỗ trợ doanh nghiệp, nhất là các doanh nghiệp khởi nghiệp sáng tạo, thúc đẩy gắn kết giữa nghiên cứu – triển khai – thương mại hóa sản phẩm.

c) Ưu tiên sử dụng các sản phẩm, giải pháp nội địa đáp ứng được các tiêu chuẩn, quy chuẩn trong các dự án, hệ thống trọng yếu nhằm vừa tạo thị trường, vừa thúc đẩy và hỗ trợ doanh nghiệp Việt Nam phát triển.

d) Xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật về mã dân sự để bảo vệ an ninh mạng.

5. Bảo đảm nguồn lực tài chính, ngân sách

Quy định an ninh mạng, bảo mật thông tin, an ninh dữ liệu là thành phần bắt buộc trong mọi dự án công nghệ thông tin; bảo đảm tỉ lệ kinh phí bình quân chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu đạt tối thiểu 15% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí. Nghiên cứu sửa đổi, bổ sung các quy định pháp luật có liên quan để tạo cơ chế thông thoáng trong đầu tư, triển khai an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

6. Bảo đảm nguồn nhân lực

a) 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.

b) 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, làm chủ công nghệ lõi trong an ninh mạng.

c) Tăng cường liên kết giữa Nhà nước – Nhà trường – Doanh nghiệp trong đào tạo, huấn luyện thực chiến. Xây dựng Mạng lưới liên kết các chuyên gia an ninh mạng trong nước và nước ngoài tham gia hỗ trợ công tác bảo đảm an ninh mạng. Mở rộng Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia.

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

IV. TỔ CHỨC THỰC HIỆN

1. Ủy ban nhân dân Thành phố

- Tổ chức quán triệt, triển khai các văn bản luật, văn bản hướng dẫn về bảo đảm an ninh mạng; tổ chức triển khai thực hiện các nhiệm vụ được giao và chủ động hướng dẫn, xử lý các vấn đề phát sinh theo chức năng, nhiệm vụ, thẩm quyền và lĩnh vực quản lý (*Nhiệm vụ thực hiện thường xuyên*).

- Chỉ đạo thực hiện việc kết nối, liên thông các hệ thống thông tin phục vụ hoạt động và chỉ đạo, điều hành (hệ thống quản lý văn bản và hồ sơ công việc, hệ thống thông tin báo cáo, hệ thống họp trực tuyến...) của các khối cơ quan Đảng, Ủy ban nhân dân Thành phố, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị -

xã hội, Tòa án nhân dân Thành phố, Viện Kiểm sát nhân dân Thành phố ***(Hoàn thành trong năm 2026).***

- Chỉ đạo việc ban hành các quy định ưu tiên sử dụng sản phẩm, dịch vụ an ninh mạng, an toàn thông tin “Make in Vietnam” đáp ứng yêu cầu bảo đảm an ninh mạng, bảo mật dữ liệu và an toàn thông tin bảo vệ an ninh mạng trong các sở, ban, ngành, địa phương ***(Nhiệm vụ thường xuyên).***

2. Đảng ủy Sở Khoa học và Công nghệ Thành phố

- Lãnh đạo, chỉ đạo Sở Khoa học và Công nghệ phối hợp Công an Thành phố, Bộ Tư lệnh Thành phố và các sở, ban, ngành, địa phương liên quan rà soát, trình cấp có thẩm quyền xem xét, điều chỉnh quy hoạch hạ tầng thông tin tổng thể từ Trung ương đến cơ sở theo hướng tập trung các máy chủ về các trung tâm dữ liệu đạt chuẩn, đủ điều kiện để triển khai đầy đủ các biện pháp bảo vệ an ninh mạng theo quy định ***(Hoàn thành trong tháng năm 2026).***

- Phối hợp Công an Thành phố triển khai TCVN 14423:2025 phù hợp với các cấp độ hệ thống thông tin theo Luật An ninh mạng số 116/2025/QH15 ***(Hoàn thành trước tháng 12/2026).***

- Chủ trì, phối hợp với các cơ quan liên quan xây dựng, trình cấp có thẩm quyền ban hành cơ chế, chính sách đặc thù thu hút và hỗ trợ các doanh nghiệp công nghệ trong nước, tạo điều kiện thuận lợi để làm chủ các công nghệ cốt lõi và phát triển các sản phẩm “Make in Vietnam” có tính đột phá, đủ sức cạnh tranh trên thị trường ***(Nhiệm vụ thường xuyên).***

3. Đảng ủy Sở Tài chính

- Chủ trì, phối hợp với các sở, ban, ngành bảo đảm kinh phí đầu tư từ ngân sách Thành phố cho hoạt động an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho các Sở, ban, ngành, địa phương.

- Phối hợp với các cơ quan liên quan điều chỉnh đồng bộ các quy định về tài chính, công sản, ngân sách, đấu thầu có liên quan để tạo thuận lợi trong quá trình triển khai thực tiễn, đáp ứng yêu cầu nhiệm vụ và đặc thù vòng đời của sản phẩm giải pháp an ninh mạng thường ngắn hơn quy định về khấu hao công sản ***(Hoàn thành trong tháng 6/2026).***

4. Các cơ quan chuyên trách tham mưu, giúp việc Đảng ủy Ủy ban nhân dân Thành phố

- Ban Tuyên giáo và Dân vận Đảng ủy: Chủ trì định hướng công tác tuyên truyền, phổ biến Chỉ thị 57-CT/TW và Chương trình hành động sâu rộng trong Đảng bộ. Chủ trì theo dõi, rà soát, phát hiện và tổ chức đấu tranh phản bác các

quan điểm sai trái, thù địch trên không gian mạng, bảo vệ nền tảng tư tưởng của Đảng.

- Văn phòng Đảng ủy: phối hợp các cơ quan, đơn vị thực hiện cập nhật, báo cáo định kỳ hằng tháng (trước ngày 25 hằng tháng) về tình hình, kết quả triển khai thực hiện Kế hoạch; gửi về Cơ quan Thường trực Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số Thành phố (Văn phòng Thành ủy) để tổng hợp, báo cáo theo quy định.

5. Cấp ủy các chi, đảng bộ cơ sở

- Các cấp ủy, tổ chức đảng, cơ quan, đơn vị triển khai thực hiện nghiêm túc Kế hoạch này. Có 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, lọt bí mật nhà nước do yếu tố chủ quan, thiếu trách nhiệm hoặc không tuân thủ quy định. Đưa vào 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 hàng năm. Triển khai chương trình đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng nhằm củng cố lòng tin của người dân trong quá trình hoạt động, tương tác và làm việc trên không gian mạng (**Nhiệm vụ thường xuyên**).

- Lãnh đạo, chỉ đạo xây dựng phương án ứng cứu sự cố an ninh mạng cho hệ thống thuộc phạm vi quản lý; triển khai tổng thể các giải pháp giám sát, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu và ứng phó xử lý sự cố (**Hoàn thành trong tháng 5/2026**).

- Lãnh đạo, chỉ đạo các cơ quan, đơn vị trực thuộc khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin thuộc phạm vi quản lý (**Hoàn thành trong tháng 6/2026**). Thực hiện xác định cấp độ hệ thống thông tin, phê duyệt cấp độ hệ thống tin đối với hạ tầng và các hệ thống thông tin đang xây dựng hoặc sẽ triển khai trong thời gian tới 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 (**Hoàn thành trong năm 2026**). Đảm bảo tích hợp đầy đủ yêu cầu về an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong toàn bộ quá trình thiết kế, thẩm định và triển khai khi xây dựng, cập nhật hoặc hoàn thiện Khung kiến trúc tổng thể quốc gia số.

- Lãnh đạo, chỉ đạo triển khai mô hình bảo đảm an toàn thông tin “4 lớp” gồm: (1) Lực lượng tại chỗ chịu trách nhiệm vận hành, giám sát và ứng cứu ban đầu khi sự cố xảy ra; (2) Hệ thống hoặc dịch vụ giám sát 24/7, giúp phát hiện sớm

các nguy cơ; (3) Đơn vị độc lập thực hiện kiểm tra, đánh giá định kỳ để đảm bảo khách quan và minh bạch; (4) 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) ***(Hoàn thành trong tháng 6/2026).***

- Đảm bảo kinh phí chi cho an toàn, an ninh mạng đạt tối thiểu 15% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí.

- Gắn kết quả thực hiện Kế hoạch với đánh giá, xếp loại mức độ hoàn thành nhiệm vụ của tập thể và cá nhân, đặc biệt là người đứng đầu.

- Kịp thời biểu dương, khen thưởng các tập thể, cá nhân có thành tích xuất sắc, các mô hình hay, cách làm sáng tạo; đồng thời xem xét, xử lý nghiêm các trường hợp không hoàn thành nhiệm vụ, thiếu trách nhiệm, gây ảnh hưởng đến các mục tiêu chung của Kế hoạch.

Nơi nhận:

- Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số Thành phố Hồ Chí Minh,
- Văn phòng Thành ủy,
- Ban Thường vụ Đảng ủy UBND Thành phố,
- Các cơ quan chuyên trách tham mưu, giúp việc Đảng ủy,
- Các chi, đảng bộ cơ sở,
- Lưu Văn phòng.

(Đính kèm kế hoạch số 34-KH/BCĐTP)

**T/M BAN THƯỜNG VỤ
PHÓ BÍ THƯ**

Nguyễn Thanh Xuân

THÀNH ỦY THÀNH PHỐ HỒ CHÍ MINH
BAN CHỈ ĐẠO VỀ PHÁT TRIỂN
KHOA HỌC, CÔNG NGHỆ, ĐỔI MỚI
SÁNG TẠO, CHUYỂN ĐỔI SỐ
THÀNH PHỐ

ĐẢNG CỘNG SẢN VIỆT NAM
TP. Hồ Chí Minh, ngày 05 tháng 5 năm 2026

Số 34 -KH/BCĐTP

KẾ HOẠCH

Triển khai thực hiện Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 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 trên địa bàn Thành phố

Căn cứ 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;

Căn cứ 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;

Căn cứ Kế hoạch số 04-KH/BCĐTW, ngày 05/01/2026 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;

Căn cứ Chương trình hành động số 13-CTrHĐ/TU ngày 30/3/2026 của 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 tại Thành phố Hồ Chí Minh;

Xét báo cáo đề nghị Đảng ủy Ủy ban nhân dân Thành phố tại Tờ trình số 1258-TTr/ĐU. ngày 06/4/2026 của Đảng ủy Ủy ban nhân dân Thành phố,

Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số Thành phố Hồ Chí Minh (*viết tắt là Ban Chỉ đạo Thành phố*) ban hành Kế hoạch triển khai thực hiện Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 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 trên địa bàn Thành phố như sau:

I. MỤC TIÊU VÀ YÊU CẦU

1. Mục tiêu

a) Trong năm 2026

- Về công tác lãnh đạo, chỉ đạo: Tạo chuyển biến mạnh mẽ về nhận thức và hành động trong toàn hệ thống chính trị và xã hội.

- **Về thể chế:** phối hợp để triển khai các quy định, hướng dẫn về khuyến khích đổi mới sáng tạo, tạo điều kiện cho doanh nghiệp mới tham gia thị trường, tiếp tục được hoàn thiện gỡ bỏ các rào cản thủ tục.

- **Về hạ tầng:** (1) Các hệ thống thông tin của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội được rà soát, khắc phục các lỗ hổng, điểm yếu an ninh mạng; (2) Các hệ thống thông tin quan trọng thuộc danh mục được ưu tiên bảo vệ của hệ thống chính trị từ cấp độ 3 trở lên (*trừ hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu*) được kết nối, chia sẻ thông tin, dữ liệu giám sát an ninh mạng 24/7 với Trung tâm An ninh mạng quốc gia (Bộ Công an); (3) Phối hợp xây dựng và ban hành các tiêu chuẩn, quy chuẩn kỹ thuật cho sản phẩm, dịch vụ an ninh mạng.

- **Nhân lực:** Nâng cao nhận thức của cán bộ, đảng viên và người dân về bảo mật thông tin, an ninh mạng và an ninh dữ liệu; Đào tạo, bồi dưỡng đội ngũ chuyên gia an ninh mạng chất lượng cao.

- **Quản trị:** Tăng cường kỷ luật, kỷ cương trong quản lý nhà nước về an ninh mạng; thực hiện quản trị an ninh mạng dựa trên đánh giá rủi ro, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật.

- **Công nghệ:** Thúc đẩy ứng dụng các công nghệ tiên tiến như trí tuệ nhân tạo, phân tích dữ liệu lớn, giám sát thông minh để phát hiện sớm và xử lý kịp thời các mối đe dọa mạng. Chuyển đổi sang mô hình phòng thủ chủ động, các giải pháp mã hóa hiện đại phục vụ bảo vệ dữ liệu quan trọng, dữ liệu bí mật và giao dịch của Nhà nước. Khuyến khích nghiên cứu, phát triển và làm chủ các công nghệ an ninh mạng thế hệ mới, tăng cường năng lực tự chủ công nghệ, hình thành hệ sinh thái công nghiệp an ninh mạng quốc gia vững mạnh.

b) Đến năm 2030

- **Thể chế:** Hoàn thiện cơ chế pháp lý để khuyến khích đổi mới sáng tạo, tạo điều kiện cho doanh nghiệp mới tham gia thị trường, sản phẩm, giải pháp an ninh mạng chất lượng có cơ hội phát triển. Các quy định của pháp luật đủ sức răn đe và phản ứng nhanh với các hành vi vi phạm pháp luật trên không gian mạng.

- **Hạ tầng:** Đưa vào vận hành hiệu quả kiến trúc bảo vệ an ninh mạng quốc gia đa lớp hiện đại, đồng bộ, hiệu quả bảo đảm chủ quyền quốc gia trên không gian mạng, bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu;

- **Nhân lực:** Đào tạo và xây dựng được đội ngũ chuyên gia an ninh mạng trình độ cao, đáp ứng nhu cầu trong nước và quốc tế.

- **Quản trị:** Triển khai và áp dụng hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia.

- **Công nghệ:** Tỉ trọng sản phẩm, dịch vụ an ninh mạng “Make in Vietnam” chiếm 50% thị trường trong nước và bắt đầu hình thành năng lực xuất khẩu đạt chuẩn quốc tế. Tự chủ nghiên cứu, sản xuất và làm chủ công nghệ lõi đối với các sản phẩm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

c) Tầm nhìn chiến lược đến năm 2045

Xây dựng nền an ninh mạng quốc gia bền vững, tự chủ, có năng lực cạnh tranh toàn cầu. Hình thành đội ngũ chuyên gia đầu ngành, nhà khoa học công nghệ số trình độ quốc tế; làm chủ các công nghệ cốt lõi, giảm phụ thuộc nhập khẩu. Phát triển hạ tầng an ninh mạng và hạ tầng số hiện đại; xây dựng các trung tâm đổi mới sáng tạo, khu công nghiệp công nghệ cao; doanh nghiệp trong nước trở thành trụ cột của ngành công nghiệp an ninh mạng Việt Nam.

2. Yêu cầu

- Kế hoạch phải được quán triệt và triển khai thống nhất trong toàn bộ hệ thống chính trị, tránh dàn trải, cục bộ, thiếu tập trung.

- Nhiệm vụ phải được tổ chức thực hiện với quyết tâm cao, có sản phẩm cụ thể, đo lường được, bảo đảm tiến độ và hiệu quả thực chất.

- Phát huy tối đa tiềm năng, trí tuệ Việt Nam, gắn với tiếp thu, làm chủ và ứng dụng hiệu quả các thành tựu công nghệ, kỹ thuật tiên tiến của thế giới.

- Gắn trách nhiệm người đứng đầu với kết quả bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; coi đây là tiêu chí quan trọng trong đánh giá, quy hoạch, bổ nhiệm cán bộ lãnh đạo, quản lý các cấp.

II. NHIỆM VỤ TRỌNG TÂM NĂM 2026

1. Kiện toàn Tiểu ban An ninh mạng Thành phố Hồ Chí Minh.

2. Các cơ quan chủ quản các cơ sở dữ liệu, hệ thống thông tin trong hệ thống chính trị Thành phố Hồ Chí Minh 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.

3. Xây dựng, đưa vào vận hành Trung tâm An ninh mạng Thành phố¹; mở rộng kết nối, chia sẻ dữ liệu giám sát, cảnh báo an ninh mạng đối với hệ thống thông tin quan trọng của hệ thống chính trị từ cấp độ 3 trở lên (trừ các hệ thống thông tin trong

¹ Kế hoạch số 133/KH-UBND ngày 20/10/2025 của Ủy ban nhân dân Thành phố về đảm bảo an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn Thành phố Hồ Chí Minh trong năm 2025.

lĩnh vực quân sự, quốc phòng và cơ yếu); 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.

4. Tham gia tích cực vào hoạt động của liên minh ứng phó sự cố an ninh mạng quốc gia nhằm bảo vệ an ninh mạng vòng ngoài cho các hệ thống thông tin, tài nguyên trọng yếu trên internet của các sở, ban, ngành, địa phương, cơ quan, doanh nghiệp trên địa bàn Thành phố.

5. Ban hành các quy định, tài liệu hướng dẫn 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 chính trị; định kỳ tổ chức kiểm tra, đánh giá việc thực hiện các quy định đảm bảo an ninh mạng, an toàn thông tin theo quy định.

6. Nghiên cứu ban hành cơ chế ưu đãi đặc biệt và chính sách ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng, bảo mật thông tin và an ninh dữ liệu “Make in Vietnam”; từng bước hình thành hệ sinh thái an ninh mạng quốc gia vững mạnh, nâng cao năng lực cạnh tranh đáp ứng nhu cầu xuất khẩu, tham gia sâu vào chuỗi giá trị toàn cầu.

7. Rà soát, trình cấp có thẩm quyền xem xét ban hành hoặc điều chỉnh quy hoạch hạ tầng công nghệ thông tin tổng thể theo hướng tập trung, chuẩn hóa Trung tâm dữ liệu. Đầu tư, nâng cấp hạ tầng công nghệ thông tin đáp ứng yêu cầu và tuân thủ quy hoạch đã được ban hành.

III. NHIỆM VỤ ĐẾN NĂM 2030

1. Nâng cao nhận thức cho toàn hệ thống chính trị và người dân

a) 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) Đổi mới mạnh mẽ nội dung, hình thức truyền thông đại chúng và trên không gian mạng; phát động phong trào thi đua “Dân vận khéo trên không gian mạng” để phổ cập kỹ năng nhận diện, phòng chống lừa đảo trực tuyến.

c) 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.

d) Triển khai các giải pháp định danh và đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng; củng cố lòng tin, trách nhiệm của người dân khi hoạt động, tương tác, làm việc trên không gian mạng.

đ) 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.

2. Xây dựng và hoàn thiện thể chế, khung pháp lý

a) Tiếp tục rà soát, sửa đổi, bổ sung, hoàn thiện hành lang pháp lý cho an ninh mạng, bảo mật thông tin, an ninh dữ liệu, bảo đảm thể chế đi trước một bước.

b) Hoàn thiện, áp dụng các tiêu chuẩn quốc gia và quy chuẩn kỹ thuật đối với các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, áp dụng trước hết đối với hạ tầng thông tin, hệ thống thông tin của các cơ quan trong hệ thống chính trị mà có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống nhân dân.

c) Xây dựng, triển khai Khung quản trị rủi ro an ninh mạng quốc gia và chỉ số đánh giá năng lực bảo đảm an ninh mạng.

d) Hoàn thiện các cơ chế trao đổi, chia sẻ thông tin trong nước và quốc tế về an ninh mạng.

3. Phát triển hạ tầng an ninh mạng hiện đại, đồng bộ, đáp ứng yêu cầu bảo vệ chủ quyền quốc gia trên không gian mạng

a) Triển khai kiến trúc bảo vệ an ninh mạng quốc gia đa lớp hỗ trợ bảo vệ cho toàn bộ hạ tầng mạng Internet và các hệ thống thông tin của các sở, ban, ngành, địa phương, tổ chức, doanh nghiệp.

b) Quy hoạch và triển khai đồng bộ các nhóm giải pháp: (i) Bảo vệ hạ tầng mạng; (ii) Bảo vệ thiết bị đầu cuối; (iii) Bảo vệ ứng dụng, dịch vụ; (iv) Bảo vệ dữ liệu; (v) Bảo vệ người dùng.

c) Bảo vệ tuyệt đối an toàn các hệ thống thông tin quan trọng, các cơ sở dữ liệu về dân cư, đất đai, tài chính, y tế, giáo dục, bảo hiểm, tư pháp,... Thiết lập cơ chế thống nhất về tiêu chuẩn, quy chuẩn bảo mật; bảo đảm an ninh mạng “ngay từ thiết kế” đối với các trung tâm dữ liệu quan trọng, các hệ thống số, nền tảng số và ứng dụng mới; khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin. Kết nối, chia sẻ dữ liệu liên thông giữa các sở, ban, ngành, địa phương trên nguyên tắc bảo mật, an toàn, đúng pháp luật, khắc phục tình trạng cát cứ, phân mảnh dữ liệu.

4. Phát triển công nghiệp an ninh mạng tự chủ và thị trường an ninh mạng cạnh tranh, minh bạch

a) Nghiên cứu xây dựng cơ chế đầu tư cho phát triển hệ sinh thái an ninh mạng, đặc biệt là hệ sinh thái “Make in Vietnam”; ưu tiên làm chủ và sản xuất nội địa các sản phẩm an ninh mạng cốt lõi, nền tảng.

b) Xây dựng thị trường cạnh tranh lành mạnh, minh bạch. Hình thành các trung tâm nghiên cứu, vườn ươm hỗ trợ khởi nghiệp và không gian đổi mới sáng tạo để hỗ trợ doanh nghiệp, nhất là các doanh nghiệp khởi nghiệp sáng tạo, thúc đẩy gắn kết giữa nghiên cứu – triển khai – thương mại hóa sản phẩm.

c) Ưu tiên sử dụng các sản phẩm, giải pháp nội địa đáp ứng được các tiêu chuẩn, quy chuẩn trong các dự án, hệ thống trọng yếu nhằm vừa tạo thị trường, vừa thúc đẩy và hỗ trợ doanh nghiệp Việt Nam phát triển.

d) Xây dựng các tiêu chuẩn, quy chuẩn kỹ thuật về mã dân sự để bảo vệ an ninh mạng.

5. Bảo đảm nguồn lực tài chính, ngân sách

Quy định an ninh mạng, bảo mật thông tin, an ninh dữ liệu là thành phần bắt buộc trong mọi dự án công nghệ thông tin; bảo đảm tỉ lệ kinh phí bình quân chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu đạt tối thiểu 15% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí. Nghiên cứu sửa đổi, bổ sung các quy định pháp luật có liên quan để tạo cơ chế thông thoáng trong đầu tư, triển khai an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

6. Bảo đảm nguồn nhân lực

a) 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.

b) 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, làm chủ công nghệ lõi trong an ninh mạng.

c) Tăng cường liên kết giữa Nhà nước – Nhà trường – Doanh nghiệp trong đào tạo, huấn luyện thực chiến. Xây dựng Mạng lưới liên kết các chuyên gia an ninh mạng trong nước và nước ngoài tham gia hỗ trợ công tác bảo đảm an ninh mạng. Mở rộng Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia.

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

IV. TỔ CHỨC THỰC HIỆN

1. Phân công trách nhiệm

a) Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số Thành phố Hồ Chí Minh

Chịu trách nhiệm chỉ đạo toàn diện việc triển khai Kế hoạch; trực tiếp cho ý kiến chỉ đạo về các chủ trương, cơ chế, chính sách lớn; chỉ đạo tháo gỡ kịp thời các

khó khăn, vướng mắc mang tính liên ngành, các điểm nghẽn vượt thẩm quyền của các sở, ban, ngành, địa phương.

b) Thường trực Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số Thành phố

Chịu trách nhiệm chỉ đạo, điều hành trực tiếp, thường xuyên quá trình tổ chức thực hiện Kế hoạch; tổ chức giao ban định kỳ với Cơ quan Thường trực Tiểu ban An ninh mạng Thành phố và các cơ quan liên quan trong việc hướng dẫn, đôn đốc, kiểm tra, giám sát tiến độ, tháo gỡ khó khăn, vướng mắc, bảo đảm Kế hoạch được triển khai đồng bộ, thống nhất, hiệu quả trong hệ thống chính trị.

c) Đảng ủy Ủy ban nhân dân Thành phố, Mặt trận Tổ quốc, các đoàn thể, tổ chức chính trị - xã hội Thành phố

- Tổ chức quán triệt, triển khai các văn bản luật, văn bản hướng dẫn về bảo đảm an ninh mạng; tổ chức triển khai thực hiện các nhiệm vụ được giao và chủ động hướng dẫn, xử lý các vấn đề phát sinh theo chức năng, nhiệm vụ, thẩm quyền và lĩnh vực quản lý (*Nhiệm vụ thực hiện thường xuyên*).

- Chỉ đạo thực hiện việc kết nối, liên thông các hệ thống thông tin phục vụ hoạt động và chỉ đạo, điều hành (hệ thống quản lý văn bản và hồ sơ công việc, hệ thống thông tin báo cáo, hệ thống họp trực tuyến...) của các khối cơ quan Đảng, Ủy ban nhân dân Thành phố, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội, Tòa án nhân dân Thành phố, Viện Kiểm sát nhân dân Thành phố (*Hoàn thành trong năm 2026*).

- Chỉ đạo việc ban hành các quy định ưu tiên sử dụng sản phẩm, dịch vụ an ninh mạng, an toàn thông tin “Make in Vietnam” đáp ứng yêu cầu bảo đảm an ninh mạng, bảo mật dữ liệu và an toàn thông tin bảo vệ an ninh mạng trong các sở, ban, ngành, địa phương (*Nhiệm vụ thường xuyên*).

d) Đảng ủy Công an Thành phố

- Chịu trách nhiệm thực hiện thống nhất quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu (*trừ lĩnh vực quân sự quốc phòng và cơ yếu*).

- Chủ trì, phối hợp với Sở Khoa học và Công nghệ thực hiện công tác giám sát, điều phối ứng phó xử lý sự cố tại địa phương; Giữ vai trò cơ quan thường trực về vấn đề bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trên địa bàn Thành phố.

- Xây dựng, vận hành Trung tâm An ninh mạng Thành phố²; kết nối, chia sẻ dữ liệu giám sát, cảnh báo an ninh mạng đến các hệ thống thông tin quan trọng thuộc

² Kế hoạch số 133/KH-UBND ngày 20/10/2025 của Ủy ban nhân dân Thành phố về đảm bảo an toàn thông tin mạng trong các cơ quan nhà nước trên địa bàn Thành phố Hồ Chí Minh trong năm 2025.

danh mục được ưu tiên bảo vệ của hệ thống chính trị từ cấp độ 3 trở lên (trừ các hệ thống tin trong lĩnh vực quân sự, quốc phòng và cơ yếu) đảm bảo hoạt động giám sát và sẵn sàng ứng phó với các nguy cơ tấn công mạng (***Hoàn thành trong năm 2026***).

- 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 theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng Bộ Công an quy định (*trừ các hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu*) (***Hoàn thành trong tháng 5/2026***). Thực hiện báo cáo về sự cố trong vòng 24 giờ nếu xảy ra và tuân theo sự điều phối ứng phó sự cố của lực lượng chuyên trách bảo vệ an ninh mạng Bộ Công an theo quy định (***Nhiệm vụ thường xuyên***).

- Phối hợp Bộ Tư lệnh Thành phố, Sở Khoa học và Công nghệ và các sở, ban, ngành: (i) Xây dựng, ban hành quy định, hướng dẫn triển khai Tiêu chuẩn Việt Nam TCVN 14423:2025 về An ninh mạng – Yêu cầu đối với hệ thống thông tin mạng quan trọng trên cơ sở hợp nhất với TCVN 11923:2017 (***Hoàn thành trước tháng 9/2026***); (ii) Tổ chức chiến dịch truyền thông sâu rộng trên truyền hình, báo chí, mạng xã hội kết hợp cảnh báo trực tiếp qua nhà mạng, ngân hàng và nền tảng số; phổ cập kỹ năng an toàn số cho người dân thông qua chương trình giáo dục, tập huấn cộng đồng và tài liệu hướng dẫn trực tuyến; xây dựng hệ thống tiếp nhận, xử lý phản ánh 24/7 liên thông giữa cơ quan chức năng, tổ chức doanh nghiệp và người dân nhằm ngăn chặn kịp thời các hình thức lừa đảo trực tuyến (***Nhiệm vụ thường xuyên***).

- Phối hợp Sở Khoa học và Công nghệ, Bộ Tư lệnh Thành phố và các cơ quan liên quan triển khai, hướng dẫn về quản lý rủi ro an ninh mạng; chỉ số đảm bảo an ninh mạng làm cơ sở đánh giá năng lực bảo đảm an ninh mạng của các sở, ban, ngành, địa phương, tổ chức, doanh nghiệp hàng năm.

- Phối hợp Sở Tài chính, Sở Khoa học và Công nghệ triển khai các quy định pháp luật về an ninh mạng, bảo mật thông tin, an ninh dữ liệu là thành phần bắt buộc trong các dự án công nghệ thông tin; bảo đảm tỷ lệ kinh phí bình quân chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, an ninh dữ liệu đạt tối thiểu 15% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí (***Nhiệm vụ thường xuyên***).

- Triển khai chương trình đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng; củng cố lòng tin, trách nhiệm của người dân khi hoạt động, tương tác, làm việc trên không gian mạng (***Nhiệm vụ thường xuyên***).

- Triển khai hiệu quả, thực chất Công ước Hà Nội về chống tội phạm mạng năm 2025 (***Nhiệm vụ thường xuyên***).

- Phối hợp với các đơn vị liên quan để tổ chức thẩm định, phê duyệt cấp độ với toàn bộ các hệ thống thông tin trọng yếu của Thành phố Hồ Chí Minh (***Nhiệm vụ thường xuyên***).

d) Đảng ủy Quân sự Thành phố

- Chịu trách nhiệm toàn diện trước Ban Thường vụ Thành ủy về công tác bảo đảm an ninh mạng, mật mã, bảo mật thông tin trong lĩnh vực quân sự, quốc phòng, cơ yếu thuộc phạm vi quản lý của Bộ Quốc phòng.

- Chỉ đạo công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo phạm vi quản lý, chức năng, nhiệm vụ được giao.

- Tổ chức triển khai các hoạt động trong công tác bảo đảm, giám sát an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với các hệ thống thông tin quân sự, quốc phòng, cơ yếu do Bộ Quốc phòng và Ban Cơ yếu Chính phủ quản lý (bao gồm cả hệ thống thông tin, dữ liệu thuộc các cơ quan, đơn vị, tổ chức, doanh nghiệp có hoạt động liên quan đến lĩnh vực quân sự, quốc phòng) (***Nhiệm vụ thường xuyên***).

- Phối hợp với các cơ quan chủ quản hệ thống thông tin quan trọng quốc gia tăng cường nguồn lực, hỗ trợ bảo vệ hệ thống thông tin, an ninh mạng, bảo mật thông tin và an ninh dữ liệu (***Nhiệm vụ thường xuyên***).

- Xây dựng và duy trì lực lượng chuyên trách đủ năng lực để thực hiện nhiệm vụ tác chiến trên không gian mạng; sẵn sàng ngăn chặn, đánh bại các cuộc tấn công mạng nhắm vào hệ thống chỉ huy, điều hành quốc phòng; tham gia bảo vệ chủ quyền quốc gia trên không gian mạng; phối hợp diễn tập các phương án đối phó với chiến tranh mạng (***Nhiệm vụ thường xuyên***).

e) Đảng ủy Sở Khoa học và Công nghệ Thành phố

- Lãnh đạo, chỉ đạo Sở Khoa học và Công nghệ phối hợp Công an Thành phố, Bộ Tư lệnh Thành phố và các sở, ban, ngành, địa phương liên quan rà soát, trình cấp có thẩm quyền xem xét, điều chỉnh quy hoạch hạ tầng thông tin tổng thể từ Trung ương đến cơ sở theo hướng tập trung các máy chủ về các trung tâm dữ liệu đạt chuẩn, đủ điều kiện để triển khai đầy đủ các biện pháp bảo vệ an ninh mạng theo quy định (***Hoàn thành trong tháng năm 2026***).

- Phối hợp Công an Thành phố triển khai TCVN 14423:2025 phù hợp với các cấp độ hệ thống thông tin theo Luật An ninh mạng số 116/2025/QH15 (***Hoàn thành trước tháng 12/2026***).

- Chủ trì, phối hợp với các cơ quan liên quan xây dựng, trình cấp có thẩm quyền ban hành cơ chế, chính sách đặc thù thu hút và hỗ trợ các doanh nghiệp công nghệ trong nước, tạo điều kiện thuận lợi để làm chủ các công nghệ cốt lõi và phát triển

các sản phẩm “Make in Vietnam” có tính đột phá, đủ sức cạnh tranh trên thị trường *(Nhiệm vụ thường xuyên)*.

g) Đảng ủy Sở Tài chính

- Chủ trì, phối hợp với các sở, ban, ngành bảo đảm kinh phí đầu tư từ ngân sách Thành phố cho hoạt động an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho các Sở, ban, ngành, địa phương.

- Phối hợp với các cơ quan liên quan điều chỉnh đồng bộ các quy định về tài chính, công sản, ngân sách, đấu thầu có liên quan để tạo thuận lợi trong quá trình triển khai thực tiễn, đáp ứng yêu cầu nhiệm vụ và đặc thù vòng đời của sản phẩm giải pháp an ninh mạng thường ngắn hơn quy định về khấu hao công sản *(Hoàn thành trong tháng 6/2026)*.

h) Ban Tuyên giáo và Dân vận Thành ủy

- Chủ trì chỉ đạo, định hướng công tác tuyên truyền, phổ biến Chỉ thị 57-CT/TW và Chương trình hành động sâu rộng trong hệ thống chính trị.

- Chủ trì theo dõi, rà soát, phát hiện và tổ chức đấu tranh phản bác các quan điểm sai trái, thù địch trên không gian mạng, bảo vệ nền tảng tư tưởng của Đảng.

i) Người đứng đầu các sở, ban, ngành, Đảng ủy, Ủy ban nhân dân các phường, xã, đặc khu

- Có 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, lọt bí mật nhà nước do yếu tố chủ quan, thiếu trách nhiệm hoặc không tuân thủ quy định. Đưa vào 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 hàng năm. Triển khai chương trình đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng nhằm củng cố lòng tin của người dân trong quá trình hoạt động, tương tác và làm việc trên không gian mạng *(Nhiệm vụ thường xuyên)*.

- Lãnh đạo, chỉ đạo đơn vị chuyên trách về công nghệ thông tin chủ trì, phối hợp Công an Thành phố xây dựng phương án ứng cứu sự cố an ninh mạng cho hệ thống thuộc phạm vi quản lý; triển khai tổng thể các giải pháp giám sát, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu và ứng phó xử lý sự cố *(trừ các hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu)* *(Hoàn thành trong tháng 5/2026)*.

- Lãnh đạo, chỉ đạo các cơ quan, đơn vị trực thuộc khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin thuộc phạm vi quản lý *(Hoàn thành trong*

tháng 6/2026). Thực hiện xác định cấp độ hệ thống thông tin, phê duyệt cấp độ hệ thống tin đối với hạ tầng và các hệ thống thông tin đang xây dựng hoặc sẽ triển khai trong thời gian tới 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 (**Hoàn thành trong năm 2026**). Đảm bảo tích hợp đầy đủ yêu cầu về an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong toàn bộ quá trình thiết kế, thẩm định và triển khai khi xây dựng, cập nhật hoặc hoàn thiện Khung kiến trúc tổng thể quốc gia số.

- Lãnh đạo, chỉ đạo triển khai mô hình bảo đảm an toàn thông tin “4 lớp” gồm: (1) Lực lượng tại chỗ chịu trách nhiệm vận hành, giám sát và ứng cứu ban đầu khi sự cố xảy ra; (2) Hệ thống hoặc dịch vụ giám sát 24/7, giúp phát hiện sớm các nguy cơ; (3) Đơn vị độc lập thực hiện kiểm tra, đánh giá định kỳ để đảm bảo khách quan và minh bạch; (4) 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) (**Hoàn thành trong tháng 6/2026**).

- Đảm bảo kinh phí chi cho an toàn, an ninh mạng đạt tối thiểu 15% trong tổng kinh phí triển khai đề án, dự án, chương trình, kế hoạch đầu tư, ứng dụng, phát triển công nghệ thông tin, bảo đảm hiệu quả, đúng quy định, tránh lãng phí.

k) Các doanh nghiệp lớn tham gia chủ trì, đồng hành trong hoạt động chuyển đổi số tại các cơ quan, đơn vị, 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. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet phải 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.

2. Kinh phí thực hiện

- 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 thêm các nguồn vốn hợp pháp khác.

- 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.

- 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.

3. Chế độ thông tin báo cáo

Các cơ quan, đơn vị, địa phương thực hiện cập nhật, báo cáo định kỳ hằng tháng (trước ngày 25 hằng tháng) về tình hình, kết quả triển khai thực hiện Kế hoạch; gửi về Cơ quan Thường trực Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số Thành phố (Văn phòng Thành ủy) để tổng hợp, báo cáo theo quy định.

4. Tổng kết, đánh giá và khen thưởng kỷ luật

- Gắn kết quả thực hiện Kế hoạch với đánh giá, xếp loại mức độ hoàn thành nhiệm vụ của tập thể và cá nhân, đặc biệt là người đứng đầu.

- Kịp thời biểu dương, khen thưởng các tập thể, cá nhân có thành tích xuất sắc, các mô hình hay, cách làm sáng tạo; đồng thời xem xét, xử lý nghiêm các trường hợp không hoàn thành nhiệm vụ, thiếu trách nhiệm, gây ảnh hưởng đến các mục tiêu chung của Kế hoạch.

- Các cấp ủy, tổ chức đảng, cơ quan, đơn vị triển khai thực hiện nghiêm túc Kế hoạch này.

Nơi nhận:

- BCD Trung ương thực hiện Nghị quyết 57 (để báo cáo),
- Văn phòng Trung ương Đảng (để báo cáo),
- Các đồng chí Thành ủy viên,
- Thành viên Ban Chỉ đạo Thành phố,
- Cơ quan chuyên trách tham mưu, giúp việc Thành ủy,
- Ủy ban Mặt trận Tổ quốc Việt Nam Thành phố, các tổ chức chính trị - xã hội Thành phố,
- Các sở, ban, ngành Thành phố,
- Đảng ủy 168 xã, phường và đặc khu thành phố và đảng ủy trực thuộc Thành ủy,
- Văn phòng Thành ủy: Lãnh đạo, các phòng chuyên môn,
- Lưu Văn phòng Thành ủy.

PHÓ BÍ THƯ

kiêm

**PHÓ TRƯỞNG BAN
THƯỜNG TRỰC BAN CHỈ ĐẠO**



Đặng Minh Thông