ỦY BAN NHÂN DÂN **THÀNH PHỐ HẢI PHÒNG**	**CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM** **Độc lập - Tự do - Hạnh phúc**
Số: 139 /KH-UBND	*Hải Phòng, ngày 17 tháng 4 năm 2026*

KẾ HOẠCH
Bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn thành phố Hải Phòng

I. CĂN CỨ LẬP KẾ HOẠCH

- Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia;

- Chỉ thị số 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;

- 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;

- Quyết định số 207-QĐ/TU ngày 28/02/2026 của Thành ủy Hải Phòng về thành lập Tiểu ban An ninh mạng thành phố Hải Phòng;

- Quyết định số 5330/QĐ-UBND, ngày 30/12/2025 của Ủy ban nhân dân thành phố về kiện toàn Ban Chỉ đạo của thành phố về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và Đề án 06;

- Quyết định số 5264/QĐ-UBND ngày 26/02/2026 của Ủy ban nhân dân thành phố về phê duyệt Chiến lược dữ liệu thành phố Hải Phòng đến năm 2030;

- Kế hoạch số 246/KH-UBND ngày 17/9/2025 của Ủy ban nhân dân thành phố về kế hoạch hành động xây dựng triển khai đồng bộ đô thị thông minh trên địa bàn thành phố Hải Phòng.

- Kế hoạch số 359/KH-UBND ngày 31/12/2025 của Ủy ban nhân dân thành phố về Chuyển đổi số thành phố Hải Phòng năm 2026;

- Kế hoạch số 49/KH-UBND ngày 12/02/2026 của Ủy ban nhân dân thành phố thực hiện Nghị quyết số 57-NQ/TW ngày 22/12/2024 của Bộ Chính trị về đột phá phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số quốc gia năm 2026;

Ủy ban nhân dân thành phố ban hành Kế hoạch bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị tại thành phố Hải Phòng, cụ thể như sau:

II. MỤC TIÊU, YÊU CẦU

1. Mục tiêu chung

Quán triệt, tổ chức triển khai thực hiện nghiêm túc, có hiệu quả các chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, trọng tâm là Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư và Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 của Ban Chỉ đạo Trung ương (BCĐ Trung ương).

Tạo sự chuyển biến sâu sắc về nhận thức và hành động trong toàn hệ thống chính trị thành phố; chuyển dịch mạnh mẽ tư duy từ "phòng thủ bị động" sang "phòng thủ chủ động, tích cực" trong công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu. Quán triệt nguyên tắc "An ninh mạng là điều kiện tiên quyết của chuyển đổi số". Chủ động triển khai đầy đủ giải pháp bảo đảm an toàn hệ thống thông tin theo cấp độ ngay từ khâu thiết kế, đầu tư, vận hành; ưu tiên các hệ thống nền tảng, hệ thống phục vụ thủ tục hành chính và hệ thống dữ liệu lõi.

Gắn kết chặt chẽ công tác bảo đảm an ninh mạng với các mục tiêu chiến lược của thành phố, xác định an ninh mạng, an ninh dữ liệu là nền tảng vững chắc, phục vụ đắc lực cho mục tiêu xây dựng Hải Phòng trở thành thành phố công nghiệp phát triển hiện đại, thông minh, bền vững. Giữ vững an ninh chính trị, trật tự an toàn xã hội trên không gian mạng, qua đó tạo môi trường số an toàn, minh bạch để thu hút đầu tư, phát triển mạnh mẽ kinh tế số, logistics và chính quyền số.

Góp phần xây dựng không gian mạng quốc gia an toàn, vững mạnh; bảo vệ an toàn tuyệt đối thông tin, bí mật nhà nước, dữ liệu của hệ thống chính trị và các hạ tầng kinh tế - xã hội trọng điểm trên địa bàn thành phố, duy trì khả năng chống chịu cao trước mọi nguy cơ tấn công mạng.

Xác định lộ trình và hiện thực hóa tầm nhìn chiến lược đến năm 2045: Xây dựng Hải Phòng trở thành địa phương đi đầu cả nước về năng lực bảo đảm an ninh mạng và an ninh dữ liệu; tự chủ về công nghệ bảo vệ hệ thống thông tin. Qua đó, kiến tạo một không gian mạng an toàn, tin cậy, làm điểm tựa vững chắc để thành phố bứt phá trong chuyển đổi số toàn diện, phát triển kinh tế số và củng cố vị thế trung tâm logistics quốc tế.

2. Mục tiêu cụ thể

2.1. Mục tiêu 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; gắn trách nhiệm giải trình trực tiếp của người đứng đầu các cơ quan, đơn vị, địa phương với kết quả bảo đảm an toàn, an ninh mạng, đưa tiêu chí an ninh mạng vào đánh giá thi đua, xếp loại cuối năm.

- Về thể chế: Góp ý, bổ sung hoàn thiện cơ chế pháp lý để 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: Xây dựng và phát triển hạ tầng an ninh mạng thành phố hiện đại, đồng bộ, đủ năng lực bảo vệ chủ quyền không gian mạng:

+ Hoàn thiện Đề án, trình cấp có thẩm quyền phê duyệt chủ trương thành lập Trung tâm An ninh mạng thành phố Hải Phòng. Trước mắt, để đáp ứng yêu cầu cấp bách, tổ chức thuê dịch vụ giám sát an ninh mạng (SOC) chuyên nghiệp đối với các hệ thống thông tin trên địa bàn thành phố đồng thời thực hiện kết nối liên thông, chia sẻ thông tin, cảnh báo rủi ro và dữ liệu giám sát 24/7 với Trung tâm An ninh mạng Quốc gia theo đúng chỉ đạo, hướng dẫn của Bộ Công an.

+ 100% các hệ thống thông tin các cơ quan Đảng, chính quyền, tổ chức chính trị, xã hội trên địa bàn thành phố phải hoàn thành phê duyệt cấp độ an toàn thông tin và triển khai đầy đủ phương án bảo vệ theo mô hình 4 lớp.

+ Tổ chức rà soát, quy hoạch và nâng cấp Trung tâm Dữ liệu thành phố theo hướng thiết lập "Nền tảng điện toán đám mây dùng riêng" của hệ thống chính trị; kiểm soát, xác thực mã hóa nghiêm ngặt 100% các giao tiếp kết nối (API) khi chia sẻ dữ liệu ra bên ngoài, đáp ứng tiêu chuẩn của Luật Dữ liệu.

+ Bảo đảm hạ tầng mật mã quốc gia hoạt động ổn định, thông suốt; triển khai đồng bộ các giải pháp bảo mật, mã hóa bằng mật mã cơ yếu phục vụ trao đổi văn bản, tài liệu mang bí mật nhà nước trên môi trường mạng từ cấp thành phố đến 100% cấp xã, phường, đặc khu.

- 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. Tổ chức nghiên cứu, rà soát, lập danh sách và triển khai thực hiện kịp thời, đầy đủ các chế độ đãi ngộ, hỗ trợ đối với lực lượng làm công tác chuyên trách về an ninh mạng, an toàn thông tin và chuyển đổi số theo quy định. Đồng thời, có cơ chế thiết thực để thu hút, giữ chân những người có chuyên môn, trình độ cao, đội ngũ chuyên gia giỏi tham gia bảo vệ, vận hành các hệ thống thông tin, cơ sở dữ liệu trọng yếu của thành phố.

- Về quản trị: Tăng cường kỷ luật, kỷ cương quản lý nhà nước, chuyển đổi phương thức từ "quản lý hành chính thuần túy" sang "quản trị dựa trên dữ liệu và rủi ro", cụ thể:

+ Siết chặt trách nhiệm giải trình của người đứng đầu các cơ quan, đơn vị; kiên quyết xử lý và hạ bậc thi đua đối với các đơn vị chậm trễ trong việc khắc phục lỗ hổng bảo mật hoặc không tuân thủ các quy định, tiêu chuẩn kỹ thuật bảo đảm an toàn, bảo mật dữ liệu.

+ Áp dụng nghiêm ngặt các quy chế quản trị dữ liệu, phân loại dữ liệu và kiểm soát quyền truy cập.

+ Triển khai quyết liệt các chiến dịch làm sạch không gian mạng địa phương; thiết lập cơ chế phối hợp rành mạch với các doanh nghiệp viễn thông, nền tảng số để xử lý triệt để tình trạng SIM rác, tài khoản ảo.

- 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 doạ mạng. Chuyển đổi sang mô hình phòng thủ chủ động, các giải pháp mã hoá 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. Nghiên cứu, phát triển và đưa vào ứng dụng các hệ thống phần mềm nội bộ nhằm tự động hóa quy trình quản lý hồ sơ nghiệp vụ, theo dõi tiến độ đánh giá an ninh mạng và cấp độ an toàn thông tin trên toàn thành phố. Ưu tiên thử nghiệm, tích hợp các mô hình trí tuệ nhân tạo (AI) vận hành độc lập, cục bộ (offline) trên máy chủ nội bộ

2.2. Mục tiêu đến năm 2030

Thành phố Hải Phòng vươn lên trở thành "pháo đài" an ninh mạng vững chắc của Vùng đồng bằng sông Hồng, bảo vệ an toàn cho hệ sinh thái kinh tế số, logistics và cảng biển, góp phần đưa Việt Nam tiếp tục được xếp hạng trong nhóm 20 quốc gia có mức đánh giá cao về Chỉ số An toàn, an ninh mạng toàn cầu (GCI). Vận hành hạ tầng thông tin quan trọng; triển khai và áp dụng hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia. Kiểm soát 100% rủi ro luồng dữ liệu liên thông tại Kho dữ liệu dùng chung (Data Lakehouse) của thành phố.

- Thể chế: Hoàn thiện cơ chế pháp lý tại địa phương 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. Cụ thể hóa các chế tài, bảo đảm 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 và Dữ liệu: 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. Bảo vệ tuyệt đối an toàn cho hạ tầng công nghệ tại các Khu kinh tế, Khu công nghiệp. Ban hành quy hoạch hạ tầng công nghệ thông tin tổng thể từ Trung ương đến địa phương, hoàn thiện toàn diện nền tảng "Đám mây dùng riêng" phục vụ toàn bộ hệ thống chính trị thành phố.

- **Nhân lực:** Đào tạo và xây dựng được đội ngũ chuyên gia an ninh mạng trình độ cao, đáp ứng nhu cầu tại địa phương và trong nước. Hình thành lực lượng nòng cốt tinh nhuệ, sắc bén, làm chủ các kỹ thuật điều tra, phục hồi chứng cứ số. Duy trì bền vững và mở rộng các chính sách đãi ngộ đặc thù nhằm thu hút, giữ chân nhân tài công nghệ cao gắn bó lâu dài với công tác an ninh mạng của thành phố.

- **Công nghệ:** Đóng góp vào tỉ trọng sản phẩm, dịch vụ an ninh mạng "Make in Vietnam" chiếm trên 50% thị trường trong nước và bắt đầu hình thành năng lực xuất khẩu đạt chuẩn quốc tế. Góp phần 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. Triển khai ứng dụng diện rộng các hệ thống tự động hóa quản trị nội bộ và các mô hình trí tuệ nhân tạo (AI) bảo đảm tính tự chủ, khép kín và an toàn tuyệt đối về thông tin nghiệp vụ.

2.3. Tầm nhìn chiến lược đến năm 2045

- **Vị thế và Chủ quyền số:** Góp phần xây dựng nền an ninh mạng quốc gia bền vững, tự chủ, có năng lực cạnh tranh cao trên trường quốc tế. Khẳng định vị thế Hải Phòng là "hạt nhân" bảo vệ chủ quyền không gian mạng của Vùng kinh tế trọng điểm Bắc Bộ; tạo lập môi trường số an toàn tuyệt đối, định hình tiêu chuẩn bảo mật quốc tế cho hệ sinh thái logistics, cảng biển thông minh và các chuỗi cung ứng toàn cầu.

- **Tự chủ Công nghệ lõi:** Làm chủ hoàn toàn các công nghệ cốt lõi mang tính chiến lược, loại bỏ sự phụ thuộc vào công nghệ và thiết bị nhập khẩu. Lực lượng chuyên trách của thành phố đạt năng lực tự nghiên cứu, phát triển và vận hành độc lập, khép kín các hệ thống phòng thủ chủ động, mạng lưới trí tuệ nhân tạo (AI) chạy cục bộ quy mô lớn, đạt đẳng cấp quốc tế.

- **Hạ tầng và Đổi mới sáng tạo:** Phát triển hạ tầng an ninh mạng và hạ tầng số hiện đại, đồng bộ. Xây dựng và mở rộng các trung tâm đổi mới sáng tạo, khu công nghiệp công nghệ cao thu hút các tập đoàn công nghệ hàng đầu thế giới đầu tư, chuyển giao công nghệ vào thành phố.

- **Nhân lực chất lượng cao:** Hình thành đội ngũ chuyên gia đầu ngành, nhà khoa học công nghệ số và lực lượng tác chiến không gian mạng trình độ quốc tế. Đưa Hải Phòng trở thành trung tâm uy tín của cả nước về đào tạo, huấn luyện thực chiến, cung cấp nguồn nhân lực tinh nhuệ và xuất khẩu các giải pháp an ninh mạng, bảo mật dữ liệu.

3. Yêu cầu

- Kế hoạch phải được quán triệt sâu sắc và triển khai thực hiện đồng bộ, thống nhất trong toàn bộ hệ thống chính trị của thành phố, kiên quyết khắc phục tình trạng dàn trải, cục bộ, hình thức, thiếu tập trung. Các nhiệm vụ, giải pháp

phải được tổ chức thực hiện với quyết tâm cao độ, tuân thủ nghiêm nguyên tắc "rõ người, rõ việc, rõ trách nhiệm, rõ tiến độ, rõ kết quả", có sản phẩm đầu ra cụ thể, có thể đo lường, giám sát, bảo đảm tiến độ và hiệu quả thực chất.

- Công tác bảo đảm an ninh mạng, an ninh dữ liệu phải gắn kết hữu cơ, chặt chẽ với Kế hoạch chuyển đổi số và Chiến lược dữ liệu của thành phố. Phải tuân thủ tuyệt đối nguyên tắc "an toàn thiết kế ngay từ đầu"; mọi dự án hạ tầng số, phần mềm, cơ sở dữ liệu dùng chung trước khi đưa vào vận hành phải được thẩm định, phê duyệt cấp độ an toàn thông tin theo quy định.

- Phát huy tối đa tiềm năng, trí tuệ tại địa phương, gắn với tiếp thu, làm chủ và ứng dụng hiệu quả các thành tựu công nghệ, kỹ thuật tiên tiến trong nước và trên thế giới. Tạo điều kiện và cơ chế thuận lợi để lực lượng chuyên trách tự nghiên cứu, phát triển, ứng dụng các công cụ tự động hóa, trí tuệ nhân tạo (AI) chạy cục bộ phục vụ nghiệp vụ chuyên sâu, bảo đảm mức độ bảo mật cao nhất đối với dữ liệu nội bộ.

- Cá thể hóa và gắn trách nhiệm trực tiếp, toàn diện của người đứng đầu cấp ủy, chính quyền, cơ quan, đơn vị, địa phương đối với kết quả bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong phạm vi quản lý. Coi đây là tiêu chí cứng, đặc biệt quan trọng trong công tác đánh giá, quy hoạch, bổ nhiệm, khen thưởng cán bộ lãnh đạo, quản lý các cấp. Xử lý nghiêm minh các trường hợp thiếu trách nhiệm, để xảy ra sự cố nghiêm trọng hoặc lộ, lọt bí mật nhà nước do nguyên nhân chủ quan.

- Bảo đảm bố trí đầy đủ, kịp thời nguồn lực để thực thi. Phấn đấu áp dụng chỉ tiêu bắt buộc phân bổ tối thiểu 15% tổng mức đầu tư của các dự án công nghệ thông tin cho an ninh mạng; đồng thời, triển khai thực hiện đầy đủ, kịp thời các cơ chế, chính sách ưu đãi, hỗ trợ để giữ chân, thu hút nguồn nhân lực chất lượng cao tham gia lực lượng chuyên trách an ninh mạng của thành phố.

III. NHIỆM VỤ TRỌNG TÂM NĂM 2026

1. Kiện toàn tổ chức và siết chặt kỷ cương, trách nhiệm người đứng đầu

Người đứng đầu các cơ quan chủ quản cơ sở dữ liệu, hệ thống thông tin chịu trách nhiệm trực tiếp, toàn diện về an ninh mạng, định kỳ và đột xuất báo cáo kết quả, mức độ tuân thủ về cơ quan thường trực. Đưa tiêu chí bảo đảm an ninh mạng vào đánh giá, xếp loại thi đua năm 2026.

2. Đầu tư Trung tâm An ninh mạng và triển khai giám sát chủ động

Đẩy nhanh tiến độ hoàn thiện Đề án, trình cấp có thẩm quyền phê duyệt chủ trương xây dựng Trung tâm An ninh mạng thành phố Hải Phòng. Trước mắt tổ chức thuê dịch vụ giám sát an ninh mạng (SOC) đối với các hệ thống thông tin

trên địa bàn thành phố; thiết lập kênh kết nối, trao đổi thông tin và chia sẻ dữ liệu giám sát 24/7 với Trung tâm An ninh mạng Quốc gia. Thiết lập các chốt kiểm soát an ninh chuyên biệt đối với Kho dữ liệu dùng chung (Data Lakehouse) và các hệ thống điều hành cảng biển, logistics.

3. Đánh giá, phê duyệt cấp độ và triển khai mô hình bảo vệ 4 lớp

Các cơ quan chủ quản tổ chức rà soát, khắc phục tổng thể các lỗ hổng an ninh mạng đối với các hệ thống thông tin theo tiêu chuẩn TCVN 14423:2025. Hoàn thành dứt điểm việc thẩm định, phê duyệt cấp độ an toàn thông tin; kiên quyết yêu cầu 100% các hệ thống thông tin trọng điểm phải triển khai mô hình bảo đảm an toàn thông tin "4 lớp" trước khi chính thức đưa vào vận hành, kết nối liên thông.

4. Nghiên cứu, phát triển phần mềm nội bộ và ứng dụng công nghệ chuyên sâu

Lực lượng chuyên trách an ninh mạng thành phố tập trung nguồn lực tự nghiên cứu, phát triển Hệ thống phần mềm quản lý nghiệp vụ, nhằm tự động hóa quy trình theo dõi, quản lý hồ sơ và đánh giá rủi ro an ninh mạng trên toàn thành phố. Ưu tiên đưa vào thử nghiệm thực chiến các mô hình trí tuệ nhân tạo (AI), bảo đảm nguyên tắc kiểm soát quyền truy cập và dữ liệu tuyệt đối không bị lộ lọt ra môi trường bên ngoài.

5. Bảo đảm nguồn lực tài chính và thực hiện chế độ đãi ngộ lực lượng chuyên trách

Rà soát, nghiên cứu bảo đảm tỷ lệ kinh phí đạt tối thiểu 15% trong tổng mức đầu tư của các dự án công nghệ thông tin để chi cho các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin. Đồng thời, khẩn trương lập danh sách và triển khai chi trả kịp thời, đầy đủ các chế độ hỗ trợ đặc thù cho cán bộ, công chức, viên chức làm công tác chuyên trách an ninh mạng theo Nghị định số 179/2025/NĐ-CP, bảo đảm giữ chân và thu hút nguồn nhân lực công nghệ cao.

6. Ưu tiên hệ sinh thái "Make in Vietnam" và làm sạch không gian mạng

Triển khai cơ chế ưu đãi đặc biệt và chính sách ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng "Make in Vietnam" đã qua kiểm định cho các cơ quan nhà nước. Phối hợp chặt chẽ với các doanh nghiệp viễn thông rà soát, xử lý triệt để SIM rác, định danh tài khoản mạng xã hội.

7. Bảo đảm an toàn thông tin từ khâu thiết kế trong các dự án Chuyển đổi số

Kiểm soát chặt chẽ yêu cầu về an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong toàn bộ quy trình thiết kế, thẩm định và triển khai khi xây dựng, cập nhật hoặc hoàn thiện kiến trúc, nền tảng số, dịch vụ công trực tuyến của thành phố, bảo đảm không để phát sinh các hệ thống công nghệ thông tin thiếu kiểm soát về mặt an ninh.

IV. 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) 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.

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 các tổ chức, cá nhân có ảnh hưởng trên không gian mạng khi có chỉ đạo, hướng dẫn của BCĐ Trung ương; 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 tham gia 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) Tham gia hoàn thiện 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 quan trọng quốc gia, 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) Tham gia xây dựng khung quản trị rủi ro an ninh mạng quốc gia và chỉ số đánh giá năng lực bảo đảm an ninh mạng.

d) Triển khai thực hiện các cơ chế trao đổi, chia sẻ thông tin trong thành phố và quốc tế về an ninh mạng khi có chỉ đạo, hướng dẫn của BCĐ Trung ương.

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 toàn diện kiến trúc bảo vệ an ninh mạng quốc gia đa lớp trên toàn bộ hạ tầng Internet và hệ thống thông tin của các cơ quan, đơn vị, địa phương. Khẩn trương quy hoạch, nâng cấp Trung tâm dữ liệu thành phố để thiết lập và vận hành "Nền tảng điện toán đám mây dùng riêng" của hệ thống chính trị, tiến tới chấm dứt việc lưu trữ phân tán, manh mún dữ liệu nhà nước trên các nền tảng thương mại thiếu an toàn.

b) Tập trung nguồn lực bảo vệ tuyệt đối an toàn cho các hạ tầng xương sống của nền kinh tế số Hải Phòng. Thiết lập vành đai bảo mật chuyên biệt và hệ thống giám sát 24/7 đối với các hệ thống điều hành Cảng biển thông minh, chuỗi cung ứng Logistics, Hải quan điện tử và hạ tầng công nghệ thông tin trọng yếu tại các Khu kinh tế, Khu công nghiệp công nghệ cao.

c) Đảm bảo an ninh mạng "ngay từ thiết kế" đối với các nền tảng số và trung tâm dữ liệu quan trọng. Áp dụng cơ chế kiểm soát truy cập nghiêm ngặt và mã hóa mức cao nhất đối với Kho dữ liệu dùng chung (Data Lakehouse) và các cơ sở dữ liệu chuyên ngành trọng điểm (cảng biển, đất đai, tài chính, y tế, giáo dục...). Kiểm soát chặt chẽ 100% các kết nối, giao diện chia sẻ dữ liệu (API) liên thông giữa các cơ quan, đơn vị, bảo đảm chia sẻ dữ liệu thông suốt, phá bỏ "cát cứ dữ liệu" nhưng tuyệt đối không để lọt lộ bí mật nhà nước. Triển khai đồng bộ 05 nhóm giải pháp: Bảo vệ hạ tầng mạng, bảo vệ thiết bị đầu cuối, bảo vệ ứng dụng/dịch vụ, bảo vệ dữ liệu và bảo vệ người dùng.

d) Tập trung nguồn lực nghiên cứu, làm chủ các công nghệ lõi chiến lược như công nghệ mật mã, thiết kế và sản xuất chip bảo mật mang thương hiệu "Make in Vietnam". Thúc đẩy nghiên cứu, phát triển và sớm đưa vào ứng dụng công nghệ mã hoá kháng lượng tử nhằm bảo vệ vững chắc các luồng dữ liệu bí mật nhà nước; khuyến khích mở rộng ứng dụng mật mã dân sự phục vụ bảo vệ an toàn thông tin, giao dịch điện tử của tổ chức, doanh nghiệp và người dân trên địa bàn.

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

a) Xây dựng và áp dụng các tiêu chí bắt buộc về việc ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng cốt lõi do doanh nghiệp trong nước làm chủ công nghệ (Make in Vietnam) đối với mọi dự án đầu tư công, hệ thống thông tin trọng yếu của thành phố. Phù hợp với chủ trương nâng cao khả năng tự chủ chiến lược của đất nước, giảm thiểu rủi ro bị cài cắm mã độc từ các thiết bị, phần mềm ngoại nhập.

b) Giao lực lượng chuyên trách đóng vai trò nòng cốt, tiên phong trong việc tự nghiên cứu, làm chủ công nghệ. Tập trung nguồn lực tự phát triển các phần mềm quản trị nội bộ; thử nghiệm, tinh chỉnh và đưa vào ứng dụng các mô hình trí tuệ nhân tạo (AI) mã nguồn mở.

c) Tận dụng lợi thế của các Khu công nghiệp, Khu kinh tế công nghệ cao tại Hải Phòng để hình thành các trung tâm nghiên cứu, vườn ươm hỗ trợ khởi nghiệp chuyên sâu về an ninh mạng và an toàn dữ liệu. Thúc đẩy mạnh mẽ việc gắn kết giữa "Nghiên cứu - Triển khai - Thương mại hoá sản phẩm", tạo điều kiện cho các doanh nghiệp công nghệ số trên địa bàn phát triển.

d) Tham gia xây dựng thị trường cạnh tranh lành mạnh, minh bạch. Gắn liền sự phát triển của công nghiệp an ninh mạng với lộ trình hình thành các nền tảng chia sẻ và Sàn giao dịch dữ liệu của thành phố; phát triển các dịch vụ đánh giá, kiểm định độc lập, triển khai các tiêu chuẩn, quy chuẩn kỹ thuật về mật mã dân sự để bảo đảm an toàn cho các luồng giao dịch số của tổ chức, doanh nghiệp và người dân.

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.

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 và ngoài thành phố tham gia hỗ trợ công tác bảo đảm an ninh mạng.

d) Tăng cường nhân lực bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho ban, ngành, địa phương theo quy định. Ưu tiên cân đối, bố trí nguồn kinh phí thường xuyên, bền vững để thực hiện chi trả đầy đủ, kịp thời các chế độ phụ cấp, hỗ trợ đặc thù cho lực lượng làm công tác chuyên trách về chuyển đổi số, an toàn thông tin mạng, an ninh mạng trên địa bàn thành phố theo quy định tại Nghị định số 179/2025/NĐ-CP.

V. TỔ CHỨC THỰC HIỆN

1. Phân công trách nhiệm

1.1 Công an thành phố

- Phát huy vai trò cơ quan thường trực Tiểu ban An ninh mạng thành phố (Tiểu ban), tăng cường công tác tham mưu Thành ủy, Ủy ban nhân dân thành phố chỉ đạo thực hiện thống nhất quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu trên địa bàn thành phố (*trừ lĩnh vực quân sự, quốc phòng và cơ yếu)*.

- Chủ trì thực hiện các nhiệm vụ sau:

+ Phối hợp các đơn vị có liên quan tham mưu Ủy ban nhân dân thành phố xây dựng Trung tâm An ninh mạng thành phố thuộc Công an thành phố; kết nối, chia sẻ dữ liệu giám sát, cảnh báo an ninh mạng đến 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 các hệ thống thông tin trong 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 (thuộc phạm vi quản lý).

Hoàn thiện báo cáo, trình cấp có thẩm quyền phê duyệt xây dựng Trung tâm An ninh mạng thành phố theo lộ trình và hướng dẫn của Bộ Công an.

Trước mắt, triển khai thuê dịch vụ giám sát an ninh mạng (SOC) cho các hệ thống thông tin cần phải bảo vệ trên địa bàn thành phố trong năm 2026 (*Hoàn thành trong quý II/2026*).

+ Tham mưu ban hành các quy định, quy trình, bộ tiêu chí và tài liệu hướng dẫn về kiểm tra, đánh giá, bảo đảm an ninh mạng, an toàn thông tin đối với các cơ sở dữ liệu, hệ thống thông tin dùng chung trong hệ thống chính trị *(thuộc phạm vi quản lý; trừ lĩnh vực quân sự, quốc phòng và cơ yếu)*; định kỳ, đột xuất tổ chức kiểm tra, đánh giá việc thực hiện các quy định về bảo đảm an ninh mạng, an toàn thông tin; tổng hợp kết quả, kiến nghị biện pháp khắc phục và báo cáo Thành ủy, Ủy ban nhân dân thành phố theo quy định.

+ Triển khai mô hình bảo đảm an toàn thông tin "4 lớp" và giám sát 24/7 đối với các hệ thống thông tin thuộc phạm vi quản lý; tăng cường kiểm tra, đánh giá độc lập định kỳ; kết nối, chia sẻ thông tin với hệ thống giám sát an ninh mạng quốc gia theo quy định, hướng dẫn của Bộ Công an.

+ Hướng dẫn, đôn đốc và phối hợp với các cơ quan, đơn vị, địa phương tổ chức rà soát, đánh giá, lập hồ sơ đề xuất và thực hiện phê duyệt cấp độ an toàn thông tin đối với các hệ thống thông tin thuộc phạm vi quản lý; 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 thực hiện phê duyệt cấp độ ATTT trước khi đưa vào vận hành chính thức. Đối với các hệ thống thông tin và hạ tầng đang sử dụng, khẩn trương hoàn thành việc rà soát, đánh giá và phê duyệt cấp độ an toàn thông tin theo đúng quy định.

+ Tổ chức triển khai, phối hợp đấu nối và vận hành các thành phần của Hệ thống phòng vệ mạng quốc gia bảo vệ vòng ngoài cho các hệ thống/tài nguyên trọng yếu trên Internet *(khi có hướng dẫn của BCĐ Trung ương).*

+ Giữ vai trò cơ quan thường trực về vấn đề bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; hướng dẫn, đôn đốc các cơ quan chủ quản hệ thống thông tin, cơ sở dữ liệu thực hiện rà soát, khắc phục tổng thể theo TCVN 14423:2025, triển khai giám sát, thực hiện chế độ báo cáo và gắn trách nhiệm người đứng đầu theo quy định.

+ Tham gia rà soát, đề xuất sửa đổi, bổ sung Luật Hình sự, pháp luật về xử lý vi phạm hành chính đủ sức răn đe, phòng ngừa xã hội và căn cứ xử lý các hành vi chưa được quy định; sửa đổi, bổ sung các quy định của pháp luật để phòng ngừa, đấu tranh, ngăn chặn và xử lý triệt để, kịp thời các hành vi vi phạm pháp luật trên không gian mạng theo chỉ đạo của Bộ Công an.

+ Phối hợp chặt chẽ với các doanh nghiệp viễn thông đẩy mạnh việc sử dụng cơ sở dữ liệu quốc gia về dân cư để định danh người dùng; tập trung xử lý dứt điểm tình trạng SIM "rác", tài khoản "ảo" và lập lại trật tự trong quản lý người dùng mạng xã hội trên địa bàn thành phố. (*nhiệm vụ thường xuyên theo hướng dẫn, chỉ đạo của Bộ Công an*).

+ Tham gia góp ý, xây dựng cơ chế hậu kiểm và đánh giá hiệu quả việc thực hiện chỉ tiêu tối thiểu 15% ngân sách cho an ninh mạng; trong đó ưu tiên sử dụng cho các sản phẩm "Make in Vietnam" đã qua kiểm định, đánh giá chất lượng. (*theo hướng dẫn của Bộ Công an).*

+ Chủ trì, phối hợp với các đơn vị có liên quan xây dựng: (1) Các khoá đào tạo thực tế về công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho cán bộ chuyên trách an ninh mạng của các đơn vị, địa phương. (2) Triển khai đào tạo, đặc biệt là phối hợp với các cơ quan truyền thông, báo chí, mạng xã hội nhằm phổ biến kiến thức an ninh mạng trên nền tảng "Bình dân học vụ số" cho người sử dụng mạng. (*nhiệm vụ thường xuyên theo hướng dẫn, chỉ đạo của Bộ Công an).*

+ Tham gia 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 theo hướng dẫn, chỉ đạo của Bộ Công an*).

+ Tuyên truyền, triển khai hiệu quả, có thực chất Công ước Hà Nội về chống tội phạm mạng năm 2025. (*nhiệm vụ thường xuyên*).

+ Tham mưu 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, Hội đồng nhân dân, Uỷ ban nhân dân, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội, Toà án nhân dân thành phố, Viện Kiểm sát nhân dân thành phố, bảo đảm an toàn và bảo mật thông tin. *(Hoàn thành trong tháng 4/2026).*

+ Tham mưu tổ chức diễn tập thực chiến quy mô cấp thành phố và thiết lập cơ chế chỉ huy, điều hành ứng phó khẩn cấp khi xảy ra các sự cố tấn công mạng nghiêm trọng nhằm vào hạ tầng trọng yếu, đặc biệt là hệ thống dữ liệu Cảng biển, Logistics và Khu kinh tế.

1.2. Sở Khoa học và Công nghệ

- Chủ trì, phối hợp Công an thành phố, Bộ Chỉ huy quân sự 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 cấp thành phố 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. *(nhiệm vụ thường xuyên).*

- Phối hợp với Công an thành phố và các cơ quan liên quan định hướng, ưu tiên bố trí kinh phí từ các chương trình, quỹ phát triển khoa học và công nghệ của thành phố cho các đề tài nghiên cứu, ứng dụng và phát triển giải pháp bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu. Đặc biệt ưu tiên phê duyệt, cấp vốn ngân sách sự nghiệp khoa học cho các nhiệm vụ tự nghiên cứu, phát triển các công cụ phần mềm quản trị nghiệp vụ nội bộ, ứng dụng trí tuệ nhân tạo (AI). *(Nhiệm vụ thường xuyên).*

1.3. Bộ Chỉ huy 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 Chỉ huy Quân sự thành phố.

- 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:

+ Theo chức năng, nhiệm vụ được giao và trong lĩnh vực thuộc phạm vi quản lý, 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 Chỉ huy quân sự thành phố và Phòng Chuyển đổi số - Cơ yếu, Văn phòng Thành ủy 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); Phối hợp với Công an thành phố xây dựng cơ chế kết nối, chia sẻ thông tin cảnh báo sớm về an ninh mạng theo chức năng, nhiệm vụ được giao. *(Nhiệm vụ thường xuyên).*

+ Tham gia xây dựng và ban hành các tiêu chuẩn, quy chuẩn kỹ thuật cho sản phẩm, dịch vụ an ninh mạng trong phạm vi quản lý.

+ 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).*

1.4. Sở Giáo dục và Đào tạo

- Phối hợp với Công an thành phố và các đơn vị có liên quan xây dựng các khoá đào tạo thực tế về công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho cán bộ chuyên trách an ninh mạng của các đơn vị, địa phương. *(Nhiệm vụ thường xuyên).*

- Chủ trì, phối hợp Công an thành phố, Bộ Chỉ huy quân sự thành phố 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". *(Nhiệm vụ thường xuyên).*

- Triển khai "Khung Năng lực số và An toàn Toàn diện" trong chương trình giáo dục phổ thông (tích hợp các kỹ năng thực hành (như nhận diện lừa đảo, quản lý danh tính số, ứng phó với bắt nạt trên mạng) vào các môn học chính khoá, giúp hình thành văn hoá số an toàn từ sớm cho thế hệ trẻ). (Theo hướng dẫn của Bộ Giáo dục và đào tạo).

1.5. Sở Tài chính

- Chủ trì, phối hợp với Ban, ngành bảo đảm kinh phí tỉ lệ 15% đầu tư từ ngân sách cho hoạt động an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho các cơ quan trong thành phố. Hướng dẫn các cơ quan ban, ngành bảo đảm kinh phí đầu tư từ ngân sách cho các hoạt động an ninh mạng, bảo mật thông tin và an ninh dữ liệu tại địa phương. *(Nhiệm vụ thường xuyên).*

- Chủ trì, phối hợp với các cơ quan liên quan nghiên cứu, đề xuất 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. (*Theo hướng dẫn của Bộ Tài chính*).

1.6. Văn phòng Ủy ban nhân dân thành phố

- Chủ trì xây dựng, đề xuất phương án kết nối, liên thông các hệ thống thông tin phục vụ hoạt động chỉ đạo, điều hành của thành phố (hệ thống quản lý văn bản và hồ sơ công việc, hệ thống thông tin báo cáo, hệ thống họp trực tuyến...) bảo đảm an toàn, bảo mật thông tin thông suốt với Chính phủ và các sở, ngành.

- Ưu tiên tham mưu triển khai sử dụng các sản phẩm, dịch vụ an ninh mạng, an toàn thông tin "Make in Vietnam" nhằm đáp ứng yêu cầu bảo vệ an ninh mạng tại cơ quan hành chính nhà nước.

1.7. Đề nghị Ban Tuyên giáo và Dân vận thành ủy chủ trì, phối hợp với các cơ quan liên quan trong thực hiện công tác tuyên truyền, phổ biến giáo dục pháp luật về bảo đảm an ninh mạng, bảo mật thông tin và 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.

1.8. Đề nghị Ủy ban Mặt trận Tổ quốc Việt Nam thành phố phát huy vai trò giám sát, phản biện xã hội của Mặt trận Tổ quốc đối với việc tổ chức thực hiện các chính sách, pháp luật, các chương trình, dự án trọng điểm về công nghệ thông tin, chuyển đổi số và an ninh mạng của thành phố.

1.9. Các sở, ban, ngành, cơ quan, địa phương

- Phối hợp với Công an thành phố chỉ đạo các cơ quan, đơn vị huy động mọi nguồn lực để khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin.

- Phối hợp với Công an thành phố tổ chức đề xuất, phê duyệt cấp độ ATTT đối với toàn bộ các hệ thống thông tin trọng yếu do mình trực tiếp quản lý, vận hành. 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, 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 tháng 4/2026).*

- Phối hợp Công an thành phố thực hiện 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 Công an thành phố theo quy định *(trừ các hệ thống thông* tin *trong lĩnh vực quân sự, quốc phòng và cơ yếu)*. 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 Công an thành phố theo quy định. *(Nhiệm vụ thường xuyên).*

- Triển khai tổng thể các giải pháp giám sát, bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu cho các hệ thống thông tin trong phạm vi quản lý trừ các hệ thống thông tin đã được thành phố giám sát. *(Hoàn thành trong tháng 4/2026).*

- 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 thành phố, bảo đảm sự phối hợp liên thông trên phạm vi toàn thành phố (trừ các hệ thống thông tin quân sự, quốc phòng, cơ yếu). *(Hoàn thành trong tháng 4/2026).*

- Phải bảo đảm tích hợp đầy đủ yêu cầu về an toàn, 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 Chính quyền số thành phố.

1.10. Người đứng đầu các cơ quan, tổ chức trong hệ thống chính trị từ cấp thành phố đến địa phương

- Cấp ủy, người đứng đầu các cơ quan, đơn vị, địa phương chịu trách nhiệm trực tiếp, toàn diện về công tác bảo đảm an ninh mạng, an ninh dữ liệu tại cơ quan, đơn vị mình.

- Tuân thủ nghiêm ngặt nguyên tắc "an toàn thiết kế ngay từ đầu" trong mọi dự án ứng dụng công nghệ thông tin; 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 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 số của người dân trong quá trình hoạt động, tương tác và làm việc trên không gian mạng. *(Nhiệm vụ thường xuyên).*

1.11. Các doanh nghiệp tại thành phố tham gia chủ trì, đồng hành trong hoạt động chuyển đổi số tại các cơ quan, đơn vị, ban, ngành, địa phương

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; tổ chức các chương trình đào tạo, tuyên truyền, bồi dưỡng kỹ năng bảo đảm an toàn thông tin, nhận diện lừa đảo trực tuyến và bảo vệ dữ liệu cá nhân cho 100% cán bộ, công nhân viên, người lao động.

Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet trong thành phố 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 kế hoạch.

- 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 báo cáo kết quả thực hiện Kế hoạch này lồng ghép vào báo cáo kết quả thực hiện Nghị quyết 57, chuyển đổi số và Đề án 06 hàng tháng của đơn vị. Giao Công an thành phố theo dõi việc thực hiện Kế hoạch này; tổng hợp, tham mưu giúp Ủy ban nhân dân thành phố báo cáo Ban Chỉ đạo Trung ương, Chính phủ, Thành ủy 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.

Yêu cầu các sở, ngành, đơn vị, địa phương liên quan triển khai thực hiện nghiêm túc Kế hoạch này./.

Nơi nhận:
- BCĐ Trung ương (Cục A05-BCA);
- TTTU, TT HĐND TP;
- UB MTTQVN TP;
- CT, các PCT UBND TP;
- Ban TG&DV TU;
- Văn phòng Thành ủy;
- Các sở, ban, ngành TP;
- UBND xã, phường, đặc khu;
- CVP, các PCVP UBND TP;
- Các phòng: NC, VX;
- Cổng TTĐT TP;
- Lưu: VT, L.Thụy.

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

Hoàng Minh Cường