

Số: /KH-SCT

Đồng Nai, ngày tháng 8 năm 2026

KẾ HOẠCH

Triển khai Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” tại Sở Công Thương

Thực hiện Kế hoạch số 184/KH-UBND ngày 27/7/2026 của Ủy ban nhân dân thành phố Đồng Nai về triển khai Đề án “Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia” trên địa bàn thành phố Đồng Nai.

Giám đốc Sở Công Thương yêu cầu Trưởng các phòng, đơn vị trực thuộc Sở tổ chức thực hiện các nội dung sau:

I. MỤC ĐÍCH, YÊU CẦU

Cụ thể hóa đầy đủ các nhiệm vụ của Kế hoạch số 184/KH-UBND thuộc phạm vi chức năng, nhiệm vụ của Sở; nâng cao năng lực phòng ngừa, phát hiện, cảnh báo, ứng phó và khắc phục sự cố an ninh mạng.

Gắn trách nhiệm của người đứng đầu với việc bảo vệ hệ thống thông tin, cơ sở dữ liệu và nền tảng số được giao quản lý; bảo đảm an ninh mạng được triển khai đồng bộ với chuyển đổi số, ứng dụng công nghệ thông tin và cải cách hành chính của Sở.

Tổ chức thực hiện có trọng tâm, đúng thẩm quyền, phù hợp điều kiện thực tế; tuân thủ quy định pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật và hướng dẫn nghiệp vụ của cơ quan có thẩm quyền; xác định rõ đầu mối, tiến độ, kết quả và tài liệu minh chứng.

II. NHIỆM VỤ, GIẢI PHÁP TRỌNG TÂM

1. Tuyên truyền, nâng cao nhận thức và trách nhiệm

Quán triệt Kế hoạch số 184/KH-UBND và các quy định về an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân đến toàn thể công chức, viên chức, người lao động; người đứng đầu phòng, đơn vị chịu trách nhiệm trong phạm vi được giao quản lý.

Triển khai phong trào “Bình dân học vụ số”, phấn đấu 100% cán bộ, đảng viên, công chức, viên chức và người lao động của Sở được trang bị kỹ năng cơ bản về an toàn thông tin, nhận diện lừa đảo trực tuyến, thư điện tử giả mạo, mã độc và hành vi lừa đảo sử dụng công nghệ cao.

Định kỳ lồng ghép nội dung thực hành an toàn trong sử dụng tài khoản, thư điện tử công vụ, thiết bị di động, chữ ký số, dữ liệu chuyên ngành và làm việc từ xa; kịp thời phổ biến các cảnh báo do Công an thành phố, Sở Khoa học và Công nghệ và cơ quan chức năng cung cấp.

Thực hiện: Thường xuyên, hằng năm.

2. Kiện toàn đầu mối và phát triển nguồn nhân lực an ninh mạng

Rà soát, lập và cập nhật danh sách cán bộ chuyên trách, bán chuyên trách về công nghệ thông tin, an toàn thông tin và cán bộ trực tiếp quản trị, vận hành các hệ thống thông tin của Sở; phân công đầu mối tiếp nhận cảnh báo và phối hợp xử lý sự cố.

Cử cán bộ tham gia đào tạo, tập huấn, diễn tập và chương trình chứng nhận kiến thức, kỹ năng chuyên sâu do cơ quan có thẩm quyền tổ chức. Cán bộ thuộc nhóm đối tượng trực tiếp quản trị, vận hành hệ thống thông tin cấp độ 3, 4, 5 (nếu có) được bồi dưỡng, cập nhật kiến thức ít nhất 01 lần/năm và đáp ứng yêu cầu chứng nhận theo quy định, hướng dẫn của cơ quan có thẩm quyền.

Xây dựng đội ngũ kế cận phù hợp vị trí việc làm, yêu cầu nhiệm vụ và khả năng cân đối nguồn lực của Sở; chủ động phát hiện, bồi dưỡng nhân sự có năng lực để tham gia mạng lưới chuyên gia an ninh mạng của thành phố theo tiêu chuẩn, chương trình đánh giá và hướng dẫn của cơ quan có thẩm quyền.

Đầu mối: Phòng Kế hoạch - Tài chính - Tổng hợp; các đơn vị quản lý, vận hành hệ thống phối hợp thực hiện.

3. Rà soát, phân loại và bảo vệ hệ thống thông tin, cơ sở dữ liệu

Rà soát, lập danh mục đầy đủ các hệ thống thông tin, cơ sở dữ liệu, nền tảng số, trang thông tin điện tử và Sàn Thương mại điện tử được giao quản lý; xác định đơn vị chủ quản, đơn vị vận hành, nguồn vốn, loại dữ liệu, hiện trạng xác định cấp độ, phương án bảo đảm an toàn và các tồn tại cần khắc phục. Hoàn thành đợt rà soát đầu trước ngày 30/9/2026; cập nhật khi có thay đổi.

Thực hiện xác định, đề xuất phê duyệt cấp độ và triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ. Đối với hệ thống sử dụng vốn ngân sách nhà nước, thực hiện bảo vệ theo mô hình 04 lớp, giám sát an toàn thông tin 24/7/365 theo mục tiêu của Kế hoạch số 184/KH-UBND; trường hợp sử dụng hạ tầng dùng chung hoặc dịch vụ thuê ngoài, phải xác định rõ trách nhiệm phối hợp, giám sát và xử lý sự cố.

Áp dụng quản lý tài khoản theo nguyên tắc tối thiểu quyền; thu hồi hoặc khóa kịp thời tài khoản không còn nhu cầu; ưu tiên xác thực nhiều yếu tố đối với tài khoản quản trị và dịch vụ quan trọng; cập nhật bản vá, phòng chống mã độc, lưu nhật ký, kiểm tra cấu hình và rà quét lỗ hổng định kỳ.

Thực hiện sao lưu dữ liệu phù hợp mức độ quan trọng của hệ thống, có bản sao tách biệt và kiểm tra khả năng phục hồi; kiểm soát việc thu thập, chia sẻ, khai thác dữ liệu, bảo đảm bí mật nhà nước, dữ liệu cá nhân và quyền, lợi ích hợp pháp của tổ chức, cá nhân.

4. Trang bị công cụ; lựa chọn, đánh giá sản phẩm, dịch vụ an ninh mạng

Căn cứ kết quả rà soát rủi ro và hiện trạng hạ tầng, đề xuất trang bị, thuê hoặc sử dụng dịch vụ tối thiểu phục vụ rà quét, phát hiện lỗ hổng; hỗ trợ điều tra số, ứng cứu và khắc phục sự cố an ninh mạng theo nhiệm vụ tại Kế hoạch số 184/KH-UBND, tránh đầu tư trùng lặp với nền tảng dùng chung của thành phố.

Ưu tiên sản phẩm, giải pháp, dịch vụ an ninh mạng “Make in Vietnam” phù hợp nhu cầu và quy định về đầu tư, mua sắm. 100% sản phẩm, dịch vụ an ninh mạng phải được kiểm định, đánh giá trước khi đưa vào sử dụng theo quy định; việc xác định danh mục và lựa chọn nhà cung cấp phải căn cứ nhu cầu thực tế, kết quả đánh giá và thẩm quyền phê duyệt.

Đầu mối: Phòng Kế hoạch - Tài chính - Tổng hợp chủ trì tổng hợp nhu cầu, tham mưu kinh phí; đơn vị được giao quản lý hệ thống xác định yêu cầu kỹ thuật và chịu trách nhiệm khai thác hiệu quả.

5. Giám sát, chia sẻ cảnh báo, ứng phó sự cố và diễn tập

Duy trì đầu mối tiếp nhận, xử lý cảnh báo; phối hợp, chia sẻ thông tin cần thiết với Công an thành phố, Sở Khoa học và Công nghệ và cơ quan chức năng theo đúng thẩm quyền, đồng thời bảo đảm yêu cầu về bí mật nhà nước, dữ liệu cá nhân và an toàn hệ thống.

Khi xảy ra hoặc có dấu hiệu sự cố, đơn vị quản lý, vận hành phải kích hoạt phương án ứng cứu; xác định phạm vi ảnh hưởng, bảo toàn chứng cứ và nhật ký; áp dụng biện pháp kỹ thuật có kiểm soát để ngăn chặn, hạn chế thiệt hại, duy trì hoặc khôi phục hoạt động thiết yếu; đồng thời báo cáo ngay Lãnh đạo Sở và Phòng Kế hoạch - Tài chính - Tổng hợp để phối hợp Công an thành phố (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) và cơ quan liên quan xử lý.

Không tự ý xóa nhật ký, dữ liệu, cài đặt lại thiết bị hoặc công khai thông tin sự cố khi chưa được người có thẩm quyền cho phép. Sau sự cố phải đánh giá nguyên nhân, khắc phục lỗ hổng, kiểm tra phục hồi và lưu hồ sơ xử lý.

Tham gia đầy đủ các cuộc diễn tập, tập huấn do Công an thành phố, Bộ Công Thương hoặc cơ quan có thẩm quyền tổ chức; định kỳ kiểm tra phương án ứng cứu, sao lưu và khôi phục tại các hệ thống do Sở trực tiếp quản lý.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện được bố trí trong dự toán ngân sách nhà nước hằng năm được cấp có thẩm quyền giao cho Sở, kinh phí dành cho khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và các nguồn kinh phí hợp pháp khác theo quy định. Các phòng, đơn vị căn cứ nhiệm vụ được giao xây dựng nội dung, dự toán gửi Phòng Kế hoạch - Tài chính - Tổng hợp để tổng hợp, tham mưu; việc quản lý, sử dụng kinh phí, đầu tư, thuê dịch vụ và mua sắm thực hiện đúng quy định, tiết kiệm, hiệu quả, không trùng lặp.

IV. TỔ CHỨC THỰC HIỆN

1. Phòng Kế hoạch - Tài chính - Tổng hợp

Là đầu mối tham mưu, theo dõi, đôn đốc và hướng dẫn triển khai; tổng hợp danh mục hệ thống, đầu mối nhân sự, nhu cầu đào tạo, trang bị công cụ và kinh phí; phối hợp tiếp nhận cảnh báo, điều phối xử lý sự cố thuộc phạm vi Sở.

Tổng hợp kết quả, tài liệu minh chứng; trình Lãnh đạo Sở báo cáo định kỳ trước ngày 05/12 hằng năm để gửi Công an thành phố (qua Phòng An ninh mạng

và phòng, chống tội phạm sử dụng công nghệ cao) trước ngày 10/12; tham mưu báo cáo đột xuất khi có yêu cầu.

2. Trung tâm Khuyến công và Tư vấn phát triển công nghiệp

Chịu trách nhiệm trực tiếp đối với Sàn Thương mại điện tử và các hệ thống thông tin được giao quản lý, vận hành; thực hiện quản lý tài khoản, cập nhật bản vá, rà quét lỗ hổng, lưu nhật ký, sao lưu, kiểm tra phục hồi, giám sát nhà cung cấp và bảo vệ dữ liệu theo cấp độ đã được phê duyệt.

Duy trì đầu mối kỹ thuật, xử lý hoặc báo cáo ngay khi phát hiện dấu hiệu bất thường; phối hợp cung cấp hồ sơ, nhật ký và thông tin cần thiết phục vụ điều tra, ứng cứu theo yêu cầu của cơ quan có thẩm quyền.

3. Các phòng, đơn vị trực thuộc Sở

Tổ chức triển khai trong phạm vi quản lý; phân công đầu mối; rà soát dữ liệu, tài khoản, quyền truy cập, thiết bị và hệ thống chuyên ngành; chấp hành quy định về bảo vệ bí mật nhà nước, dữ liệu cá nhân, sử dụng thư điện tử công vụ, chữ ký số và thiết bị công nghệ thông tin.

Gửi kết quả thực hiện và tài liệu minh chứng về Phòng Kế hoạch - Tài chính - Tổng hợp trước ngày 30/11 hằng năm; báo cáo ngay khi phát sinh sự cố, nguy cơ hoặc yêu cầu đột xuất; chịu trách nhiệm về tính chính xác của thông tin báo cáo.

Yêu cầu Trưởng các phòng, đơn vị trực thuộc Sở nghiêm túc triển khai thực hiện. Trong quá trình thực hiện, nếu có khó khăn, vướng mắc, kịp thời báo cáo Lãnh đạo Sở (qua Phòng Kế hoạch - Tài chính - Tổng hợp) để xem xét; trường hợp vượt thẩm quyền, tổng hợp báo cáo Ủy ban nhân dân thành phố (qua Công an thành phố) theo quy định./.

GIÁM ĐỐC

Nơi nhận:

- Như trên;
- Công an thành phố Đồng Nai;
- Giám đốc và các Phó Giám đốc;
- Các phòng, đơn vị trực thuộc Sở Công Thương;
- Lưu: VT, KHTCTH.

Vũ Ngọc Long