

**ỦY BAN NHÂN DÂN
THÀNH PHỐ ĐỒNG NAI**

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

Số: /UBND-NC

Đồng Nai, ngày tháng 5 năm 2026

V/v tăng cường công tác đảm bảo
an ninh mạng, an toàn thông tin

Kính gửi:

- Công an tỉnh;
- Các Sở, ban, ngành;
- UBND các phường, xã;
- Các doanh nghiệp trên địa bàn thành phố.

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; 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 kế hoạch bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị;

Thực hiện Kế hoạch số 04-KH/BCĐ ngày 13/3/2026 của Ban chỉ đạo phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số về việc triển khai thực hiện bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn thành phố Đồng Nai.

Ngày 14/11/2025, Ủy ban nhân dân tỉnh Đồng Nai đã ban hành Công văn số 463/UBND-NC về việc tăng cường đảm bảo an toàn, an ninh mạng, bảo mật dữ liệu cho các hệ thống thông tin. Đến nay, các đơn vị trên địa bàn thành phố đã quán triệt, thực hiện nghiêm túc các nhiệm vụ được giao cụ thể như: Cơ bản hoàn thành việc xác định cấp độ hệ thống thông tin, triển khai các phương án bảo đảm an ninh, an toàn thông tin theo cấp độ, triển khai tốt các biện pháp phòng chống mã độc... Tuy nhiên hiện nay, hoạt động tấn công mạng, gián điệp mạng trên địa bàn cả nước nói chung và trên địa bàn thành phố Đồng Nai nói riêng đang diễn biến phức tạp, đặc biệt là hình thức tấn công mã hóa dữ liệu đòi tiền chuộc đang được các đối tượng xấu triệt để lợi dụng để tấn công vào các cơ sở dữ liệu, hệ thống thông tin quan trọng, cơ sở hạ tầng trọng yếu trên các lĩnh vực như tài chính, y tế, giáo dục gây thiệt hại lớn về kinh tế và ảnh hưởng đến uy tín của cơ quan, tổ chức, doanh nghiệp. Trong khi đó các cơ quan, tổ chức, doanh nghiệp chưa triển khai đầy đủ các phương án bảo đảm an ninh mạng, an toàn thông tin theo quy định.

Để chủ động trong công tác, kịp thời ứng phó với các sự cố mất an toàn thông tin; Chủ tịch UBND thành phố đề nghị:

1. Thủ trưởng các Sở, ban, ngành và các đơn vị trực thuộc; Chủ tịch UBND các xã, phường

- Tăng cường công tác triển khai, quán triệt thực hiện các quy định của pháp luật, các chỉ thị, nghị quyết, chương trình và kế hoạch của cấp trên về công tác đảm bảo an ninh mạng, an toàn thông tin; quán triệt quan điểm bảo đảm an ninh mạng, an ninh dữ liệu là yếu tố nền tảng, yêu cầu bắt buộc ngay từ khâu quy hoạch, thiết kế, xây dựng, vận hành hệ thống thông tin trong phạm vi quản lý, coi đây là nhiệm vụ chiến lược để bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng. Trường hợp xảy ra sự cố tấn công mạng cần kịp thời báo cáo về cơ quan chủ quản và tuân thủ sự điều phối ứng cứu sự cố của cơ quan chuyên trách về an ninh mạng.

- Khẩn trương rà soát, cập nhật, hoàn thiện hồ sơ đề xuất cấp độ theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ cho 100% hệ thống thông tin thuộc phạm vi quản lý (*kể cả các đơn vị trực thuộc đặc biệt trong lĩnh vực y tế, giáo dục...*) trình cấp có thẩm quyền thẩm định, phê duyệt.

- Đảm bảo 100% máy tính của đơn vị phải được cài đặt phần và sử dụng giải pháp phòng chống mã độc tập trung theo hướng dẫn của Công an tỉnh tại Công văn số 2818/CAT-PA05 ngày 21/11/2025, đảm bảo hoàn **thành trước ngày 15/6/2026**.

- Thủ trưởng các Sở, ban, ngành và các đơn vị trực thuộc; Chủ tịch UBND các xã, phường chỉ đạo các đơn vị cam kết đảm bảo an ninh, an toàn và bảo mật trong kết nối đến Cơ sở dữ liệu quốc gia về dân cư theo Công văn số 5846/UBND-NC ngày 22/9/2025 của UBND tỉnh và Công văn 1766/CAT-PA05 ngày 03/10/2025 của Công an tỉnh.

- Ban hành quy chế và các quy trình vận hành, sửa chữa, thay thế thiết bị công nghệ thông tin; đảm bảo các thiết bị trước khi đưa vào sử dụng phải được kiểm tra, đánh giá an toàn thông tin; xây dựng các phương án ứng phó sự cố, đảm bảo an toàn thông tin mạng tại đơn vị; đảm bảo 100% hệ thống thông tin phải được triển khai đầy đủ phương án bảo đảm an ninh mạng theo cấp độ đã phê duyệt đáp ứng các tiêu chuẩn quốc gia TCVN 11930:2017, TCVN 14423:2025 (*Kèm theo các phương án bảo đảm an ninh mạng theo cấp độ*) nhất là phương án sao lưu dữ liệu tuân thủ quy tắc 3-2-1 đó là: 03 bản sao, lưu trữ trên 02 loại phương tiện khác nhau với 01 bản lưu ngoại tuyến.

- Người đứng đầu phải trực tiếp chỉ đạo, chịu trách nhiệm trước pháp luật và Chủ tịch UBND thành phố nếu để hệ thống thông tin thuộc phạm vi quản lý bị xâm nhập, mất an toàn thông tin hoặc lộ lọt bí mật nhà nước do thiếu trách nhiệm trong công tác bảo vệ.

2. Công an thành phố (Cơ quan chuyên trách về đảm bảo an toàn thông tin mạng trên địa bàn thành phố)

- Chủ trì triển khai đồng bộ, quyết liệt các giải pháp, nhiệm vụ về đảm bảo an toàn thông tin mạng, phối hợp chặt chẽ với các đơn vị vận hành hệ thống thông tin trên địa bàn thành phố nắm bắt lộ trình tích hợp các hệ thống thông tin sau sáp nhập để điều chỉnh quy mô, phạm vi giám sát an ninh mạng, bảo đảm nguyên tắc các hệ thống thông tin quan trọng phải được giám sát bao gồm cả hệ thống cũ còn tiếp tục sử dụng, khai thác hồ sơ, dữ liệu sau hợp nhất.

- Phối hợp với Văn phòng UBND thành phố, Sở Khoa học và Công nghệ rà soát, tài khoản người dùng tại các đơn vị có kết nối Cổng dịch vụ công; rà soát thiết bị đầu cuối phục vụ giải quyết thủ tục hành chính để triển khai, bổ sung giải pháp phòng chống mã độc tập trung (EDR) theo quy định.

- Yêu cầu các đơn vị có Trung tâm tích hợp dữ liệu, các hệ thống quan trọng thuộc danh mục cần ưu tiên bảo vệ (hệ thống thông tin y tế, giáo dục, xử lý thủ tục hành chính...) thực hiện kết nối, chia sẻ dữ liệu giám sát về Trung tâm an ninh mạng quốc gia để hỗ trợ giám sát, điều phối ứng phó sự cố. Duy trì giám sát 24/7 đối với toàn bộ các hệ thống thông tin và cập nhật dữ liệu cảnh báo về Trung tâm an ninh mạng quốc gia (**hoàn thành trong tháng 6/2026**).

- Giao Công an thành phố triển khai Công văn này đến các cơ quan, tổ chức, doanh nghiệp trên địa bàn thành phố.

- Định kỳ, đột xuất thực hiện kiểm tra, đánh giá an toàn, an ninh mạng theo hồ sơ đề xuất cấp độ tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và rà soát, thực hiện sẵn lòng mỗi nguy hại, khắc phục các điểm yếu, lỗ hổng bảo mật theo quy định của pháp luật, trọng tâm là việc xây dựng các phương án bảo đảm an ninh mạng, an toàn thông tin, các thiết bị mạng, máy chủ, các thiết bị đầu cuối tại các đơn vị có xử lý và lưu trữ dữ liệu lớn của người dân và các doanh nghiệp trên địa bàn thành phố Đồng Nai.

3. Văn phòng UBND thành phố

Chủ động kiểm tra, đánh giá an toàn thông tin hệ thống thông tin Trung tâm Phục vụ hành chính công thành phố khắc phục triệt để sơ hở, tồn tại, hạn chế về bảo đảm an ninh mạng, an toàn hệ thống thông tin, qua kiểm tra, đánh giá; quản lý chặt chẽ, áp dụng đầy đủ các biện pháp bảo mật nhằm ngăn ngừa nguy cơ lộ, mất hoặc bị chiếm quyền tài khoản người dùng.

4. Sở Khoa học và Công nghệ

- Phối hợp với doanh nghiệp cung cấp dịch vụ viễn thông, Internet, an toàn thông tin mạng, công nghệ thông tin tại địa phương thành lập tổ thường trực, bố trí lực lượng giám sát 24/7 cho các hệ thống dịch vụ công, hệ thống thông tin phục vụ chỉ đạo, điều hành theo cam kết, hợp đồng đã ký kết; kịp thời phát hiện, ứng phó các sự cố an ninh mạng, an toàn thông tin.

- Chỉ đạo đơn vị, doanh nghiệp ký hợp đồng cung cấp dịch vụ vận hành Công Dịch vụ công giải quyết thủ tục hành chính; hệ thống quản lý và điều hành Đồng Nai-S triển khai đầy đủ giải pháp bảo đảm an toàn thông tin mạng cấp độ 3; đồng thời quản lý chặt chẽ API kết nối Công Dịch vụ công thành phố với Cơ sở dữ liệu quốc gia về dân cư, tuân thủ đúng quy định về bảo mật, an toàn thông tin.

- Đối với các hệ thống thông tin dịch chuyển, tích hợp lên Trung tâm Dữ liệu quốc gia (theo Kế hoạch số 75/KH-UBND ngày 08/02/2026 của UBND tỉnh) chủ động phối hợp Công an thành phố trong công tác giám sát, đảm bảo an toàn thông tin, bảo mật dữ liệu theo đúng quy định (Công văn số 1433/CAT-PA05 ngày 01/4/2026 của Công an tỉnh).

- Chủ động phối hợp các đơn vị liên quan xây dựng hồ sơ đề xuất cấp độ an toàn thông tin, trình cấp có thẩm quyền phê duyệt đối với các hệ thống thông tin phục vụ chuyên đổi số trên địa bàn thành phố thuộc phạm vi quản lý, vận hành theo quy định của pháp luật.

5. Sở Tài chính

Căn cứ khả năng cân đối ngân sách, tham mưu cấp có thẩm quyền bố trí (hỗ trợ) kinh phí để bảo đảm an toàn, an ninh mạng theo chỉ đạo Ban Chấp hành Trung ương tại Chỉ thị số 57-CT/TW ngày 31/12/2025 về tăng cường bảo đảm an ninh mạng, an toàn thông tin, an ninh dữ liệu trong hệ thống chính trị.

6. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet

Nghiên cứu, triển khai các giải pháp trên thiết bị truy cập Internet do doanh nghiệp cung cấp cho người sử dụng nhằm bảo vệ người sử dụng không truy cập vào các nguồn thông tin vi phạm pháp luật và ngăn chặn nguy cơ mất an toàn thông tin mạng; thực hiện kết nối, chia sẻ thông tin, dữ liệu theo hướng dẫn của Bộ Khoa học và Công nghệ.

7. Đối với các doanh nghiệp trên địa bàn thành phố

Khuyến nghị các tổ chức, doanh nghiệp trên địa bàn thành phố ban hành quy chế đảm bảo an ninh mạng cho cơ quan đơn vị; xây dựng hồ sơ cấp độ an toàn thông tin theo Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ; Phương án bảo đảm an ninh mạng theo cấp độ đáp ứng các tiêu chuẩn quốc gia TCVN 11930:2017, TCVN 14423:2025 (*Kèm theo các phương án bảo đảm an ninh mạng theo cấp độ*) nhất là phương án sao lưu dữ liệu tuân thủ quy tắc 3-2-1 đó là: 03 bản sao, lưu trữ trên 02 loại phương tiện khác nhau với 01 bản lưu ngoại tuyến và giải pháp phòng chống mã độc cho thiết bị máy tính đầu cuối của Công ty nhà nước, tổ chức, doanh nghiệp trên địa bàn thành phố Đồng Nai.

Nhận được Công văn này, đề nghị các cơ quan, đơn vị, tổ chức, doanh nghiệp trên địa bàn thành phố khẩn trương triển khai thực hiện; trong quá trình

triển khai thực hiện có khó khăn, vướng mắc, các đơn vị báo cáo về UBND thành phố (qua Công an thành phố - Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao; đồng chí Thượng tá Trương Minh Trung, email: trungtm.cat@dongnai.gov.vn số điện thoại: 0938018280) để phối hợp, thực hiện./.

Nơi nhận:

- Như trên;
- CT, các PCT UBND thành phố;
- Chánh, các PCVP UBND thành phố;
- Lưu: VT, KGVX, NC.

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**

Lê Trường Sơn