ỦY BAN NHÂN DÂN TỈNH ĐỒNG NAI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 200 /KH-UBND	*Đồng Nai, ngày 17 tháng 4 năm 2026*

KẾ HOẠCH
Triển khai công tác đảm bảo an ninh mạng trên địa bàn tỉnh Đồng Nai năm 2026

Căn cứ Luật An ninh mạng ngày 10/12/2025;

Căn cứ Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Nghị định số 05/2017/NĐ-CP ngày 16/3/2017 của Chính phủ quy định về hệ thống phương án ứng cứu khẩn cấp đảm bảo an toàn thông tin mạng quốc gia;

Căn cứ Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030;

Căn cứ Chỉ thị số 14/CT-TTg ngày 25/05/2018 của Thủ tướng Chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại; Chỉ thị số 18/CTTTg ngày 13/10/2022 của Thủ tướng Chính phủ về đẩy mạnh triển khai các hoạt động ứng cứu sự cố an toàn thông tin mạng Việt Nam; Chỉ thị số 09/CT-TTg ngày 23 tháng 02 năm 2024 của Thủ tướng Chính phủ về tuân thủ quy định pháp luật và tăng cường bảo đảm an toàn hệ thống thông tin theo cấp độ;

Căn cứ Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thông quy định hoạt động giám sát an toàn hệ thống thông tin; Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01 tháng 7 năm 2016 về bảo đảm an toàn hệ thống thông tin theo cấp độ.

Căn cứ Quyết định số 146/QĐ-TTg ngày 28/01/2022 của Thủ tướng Chính phủ phê duyệt Đề án "Nâng cao nhận thức, phổ cập kỹ năng và phát triển nguồn nhân lực chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030".

UBND tỉnh Đồng Nai ban hành Kế hoạch triển khai công tác đảm bảo an ninh mạng trên địa bàn tỉnh năm 2026 như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Nâng cao năng lực về bảo đảm an toàn, an ninh mạng, chủ động sẵn sàng

Địa chỉ: Số 02, đường Nguyễn Văn Trị, phường Trấn Biên, tỉnh Đồng Nai.
SĐT: (0251) 3822501 – FAX: (0251) 3823854 – 3824934.

ứng phó với các nguy cơ, thách thức từ không gian mạng nhằm bảo vệ vững chắc chủ quyền, lợi ích, quốc phòng, an ninh quốc gia, trật tự an toàn xã hội, bảo vệ chủ quyền quốc gia trên không gian mạng và công cuộc chuyển đổi số quốc gia, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

- Xây dựng hệ thống đảm bảo an ninh toàn diện, vững chắc, đáp ứng các tiêu chuẩn và quy định của pháp luật, bảo vệ hiệu quả các hệ thống thông tin phục vụ hoạt động của chính quyền số, kinh tế số, xã hội số trên địa bàn.

- Nâng cao năng lực đảm bảo an ninh mạng cho toàn bộ hạ tầng, hệ thống thông tin, dữ liệu tại Trung tâm tích hợp dữ liệu trên địa bàn tỉnh.

- Hạ tầng và trang thiết bị an toàn thông tin được đánh giá, phát hiện sớm các lỗ hổng bảo mật, nguy cơ có thể ảnh hưởng đến hạ tầng mạng để có biện pháp khắc phục, xử lý sự cố kịp thời, hiệu quả.

2. Yêu cầu

- Mỗi cơ quan, đơn vị, đặc biệt là người đứng đầu cơ quan, đơn vị phải nhận thức đúng đắn, toàn diện và tổ chức thực hiện nghiêm túc, có hiệu quả các quan điểm, yêu cầu, chỉ đạo của cấp trên trong công tác đảm bảo an ninh mạng trên địa bàn tỉnh; đảm bảo thực hiện đúng quy định của pháp luật.

- Xác định từng công việc cụ thể, phân công trách nhiệm rõ ràng, phù hợp với chức năng, nhiệm vụ được giao; thực thi tốt cơ chế phối hợp giữa các cơ quan, đơn vị trong quá trình thực hiện đảm bảo an ninh mạng.

II. PHẠM VI VÀ ĐỐI TƯỢNG ÁP DỤNG

1. Phạm vi

Các Sở, ban, ngành và đơn vị trực thuộc; các đơn vị sự nghiệp công lập; UBND các xã, phường và các doanh nghiệp trên địa bàn tỉnh Đồng Nai.

2. Đối tượng

- Cơ sở hạ tầng kỹ thuật phục vụ Chính quyền điện tử/Chính quyền số (Trung tâm dữ liệu, mạng truyền số liệu chuyên dùng, mạng LAN nội bộ).

- Các Hệ thống thông tin (HTTT) dùng chung và chuyên ngành của tỉnh.

- Các hệ thống thông tin của các Sở, ban, ngành và đơn vị trực thuộc; UBND các xã, phường; các đơn vị sự nghiệp công lập; các doanh nghiệp trên địa bàn tỉnh Đồng Nai.

- Cán bộ, công chức, viên chức và người lao động tham gia vận hành, sử dụng hệ thống thông tin.

III. NỘI DUNG THỰC HIỆN

1. Quán triệt, nâng cao nhận thức, hành động trong công tác đảm bảo an toàn, an ninh mạng của cán bộ, công chức, viên chức, lực lượng vũ trang; đẩy mạnh tuyên truyền, vận động các tầng lớp nhân dân nắm rõ tầm quan trọng của việc đảm bảo an toàn, an ninh mạng và vận động người dân chung tay, góp sức

thực hiện đảm bảo an toàn thông tin trên địa bàn tỉnh được an toàn, hiệu quả. Quán triệt nguyên tắc người đứng đầu cơ quan, đơn vị chịu trách nhiệm trước Chủ tịch UBND tỉnh nếu để xảy ra việc mất an toàn, an ninh mạng, lộ lọt bí mật nhà nước tại cơ quan, đơn vị mình quản lý.

2. Phân loại, xác định, phê duyệt hồ sơ đề xuất cấp độ và triển khai đầy đủ các biện pháp bảo đảm an toàn thông tin theo phương án được phê duyệt trong Hồ sơ đề xuất cấp độ

- Rà soát, hướng dẫn, đôn đốc, cập nhật lại và trình phê duyệt Hồ sơ đề xuất cấp độ đối với hệ thống thông tin của các Sở, ban, ngành, UBND các phường, xã và các đơn vị sự nghiệp công lập trên địa bàn tỉnh.

- Đầu tư, nâng cấp trang thiết bị, bản quyền phần mềm, thiết lập cấu hình hệ thống đáp ứng đầy đủ các yêu cầu an toàn theo phương án được phê duyệt trong hồ sơ đề xuất cấp độ như: các thiết bị lõi, thiết bị tường lửa, thiết bị mạng, hệ thống phòng chống mã độc.

3. Tổ chức bảo đảm an toàn thông tin theo mô hình 4 lớp

3.1. Nâng cao năng lực lực lượng tại chỗ

- Đào tạo, tuyển dụng hoặc thuê chuyên gia, bảo đảm mỗi đơn vị chuyên trách an toàn thông tin mạng có tối thiểu 05 chuyên gia an ninh mạng.

- Tổ chức tối thiểu 01 cuộc diễn tập thực chiến an ninh mạng trong năm. Trong đó, đảm bảo có tổ chức diễn tập thực chiến 01 lần/năm các hệ thống thông tin cấp độ 3 trở lên.

- Phân công, bố trí cụ thể cán bộ chuyên trách an ninh mạng tại các đơn vị, địa phương bảo đảm đáp ứng khả năng quản lý, vận hành và xử lý các sự cố cơ bản về an toàn thông tin.

- Định kỳ hàng năm triển khai các khóa đào tạo, bồi dưỡng kỹ thuật về an ninh mạng cho cán bộ chuyên trách/kiêm nhiệm về an toàn thông tin; các lớp cho cán bộ vận hành hệ thống, kỹ năng bảo mật và xử lý các sự cố về an toàn, an ninh mạng; Tổ chức tập huấn chuyên sâu các quy định về an toàn thông tin, hướng dẫn triển khai bảo đảm an ninh mạng theo cấp độ, hướng dẫn triển khai một số phương án ứng cứu, khắc phục sự cố an ninh mạng.

3.2. Tổ chức giám sát bảo vệ

- Phấn đấu 100% hệ thống thông tin của cơ quan, tổ chức được tổ chức bảo đảm an ninh mạng thực chất, toàn diện; hoàn thành mở rộng phạm vi giám sát, bảo vệ cho 100% hệ thống thông tin thuộc phạm vi quản lý. Đối với các hệ thống thông tin cấp độ 3 trở lên phải tổ chức giám sát, bảo vệ đầy đủ các lớp: lớp mạng, lớp ứng dụng, lớp cơ sở dữ liệu, lớp thiết bị đầu cuối.

- Tăng cường năng lực phòng chống phần mềm độc hại sử dụng các giải pháp, phần mềm đáp ứng các yêu cầu kỹ thuật tối thiểu bao gồm: Có chức năng

cho phép quản trị tập trung; có dịch vụ, giải pháp hỗ trợ kỹ thuật 24/7, có khả năng phản ứng kịp thời trong việc phát hiện, phân tích và gỡ bỏ phần mềm độc hại; có thể chia sẻ thông tin, dữ liệu thống kê tình hình lây nhiễm mã độc với hệ thống kỹ thuật của cơ quan chức năng có thẩm quyền, tuân thủ theo tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Công an và các quy định của pháp luật.

- Tiếp tục quản lý và duy trì hoạt động của 02 hệ thống (Trung tâm điều hành an ninh mạng (SOC) và hệ thống phòng chống mã độc EDR) đồng thời khẩn trương xây dựng Trung tâm An ninh mạng cấp tỉnh nhằm tăng cường năng lực bảo đảm an toàn, an ninh mạng hỗ trợ hiệu quả công tác phòng ngừa, phát hiện và xử lý các hành vi vi phạm pháp luật liên quan đến an ninh mạng, an ninh quốc gia và trật tự an toàn xã hội.

- Tổ chức giám sát 24/7 các hệ thống thông tin trên địa bàn tỉnh, thường xuyên theo dõi, thống kê chỉ số lây nhiễm mã độc trên các thiết bị đầu cuối, các hệ thống thông tin trong phạm địa phương để có giải pháp kịp thời các nguy cơ gây mất an ninh mạng.

3.3. Kiểm tra, đánh giá an toàn thông tin các hệ thống trên địa bàn tỉnh

- Kiểm tra, đánh giá việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Kiểm tra, đánh giá hiệu quả của các biện pháp bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin được phê duyệt.

- Tổ chức rà soát danh sách các trang website (.gov.vn) bao gồm cả các subdomain để kiểm tra, đánh giá phát hiện mã độc, lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống thông tin trên địa bàn tỉnh.

3.4. Kết nối, chia sẻ dữ liệu

Duy trì kết nối ổn định, chia sẻ đầy đủ dữ liệu giám sát theo thời gian thực về Trung tâm An ninh mạng quốc gia để được hỗ trợ giám sát, phân tích, cảnh báo sớm các nguy cơ về an ninh mạng và tấn công mạng.

4. Tổ chức triển khai phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng

- Kiện toàn Đội ứng cứu sự cố an toàn thông tin mạng tỉnh Đồng Nai trên cơ sở Quyết định số 1173/QĐ-UBND ngày 05/9/2025 của UBND tỉnh bảo đảm hoạt động ứng cứu sự cố ATTT mạng phải chuyển từ bị động sang chủ động, bao gồm: Chủ động thực hiện săn lùng mối nguy hại và rà quét lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý.

- Tiếp tục thực hiện nghiêm túc, hiệu quả Kế hoạch số 79/KH-UBND tỉnh ngày 05/9/2025 của UBND tỉnh về việc Ứng phó sự cố, bảo đảm an toàn thông tin mạng trên địa bàn tỉnh Đồng Nai trong đó các đơn vị, địa phương thành lập

các tổ ứng cứu sự cố nội bộ gồm: 01 đầu mối điều phối; 01 cán bộ kỹ thuật phụ trách an toàn thông tin; 01 cán bộ phụ trách quản lý các hệ thống, ứng dụng.

IV. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh

- Chủ trì, phối hợp với Sở Khoa học và Công nghệ thường xuyên rà soát, đánh giá tổng thể về an ninh mạng theo quy định của Chính phủ và hướng dẫn của Bộ Công an; phân loại, xác định cấp độ an toàn hệ thống thông tin và xây dựng phương án đảm bảo an toàn hệ thống thông tin theo cấp độ phù hợp với quy định của pháp luật. Báo cáo đầy đủ, kịp thời về tình hình đảm bảo an ninh mạng tại cơ quan, đơn vị, địa phương theo định kỳ hoặc khi có yêu cầu; đào tạo, huấn luyện, diễn tập nâng cao trình độ, kỹ năng cho đội ngũ nhân lực giám sát an ninh mạng cho người dùng và cán bộ liên quan đến các hệ thống thông tin của các sở, ban, ngành, UBND các xã, phường trên địa bàn tỉnh.

- Tham mưu đầu tư, triển khai các giải pháp bảo đảm an toàn hạ tầng mạng, máy chủ, ứng dụng, dữ liệu cho Trung tâm tích hợp dữ liệu và các hệ thống thông tin trên địa bàn tỉnh; đồng thời, triển khai các giải pháp phòng chống mã độc tấn công, xâm nhập hệ thống máy tính, hệ thống thông tin, cơ sở dữ liệu chuyên ngành cho các cơ quan, đơn vị; đảm bảo an ninh an toàn thông tin trong quá trình dịch chuyển, tích hợp hệ thống thông tin của tỉnh lên Trung tâm Dữ liệu quốc gia.

- Phối hợp với Sở Khoa học và Công nghệ tuyên truyền tổ chức hội thi nâng cao nhận thức Chuyển đổi số, An toàn thông tin, Blockchain, Trí tuệ nhân tạo, phát triển dữ liệu cho cán bộ công chức, viên chức, người dân trên địa bàn tỉnh năm 2026. Thường xuyên kiểm tra, rà soát xử lý, khắc phục các lỗ hổng, điểm yếu về bảo mật các hệ thống thông tin của các Sở, ban, ngành, UBND các phương, xã trên địa bàn tỉnh.

- Chủ động phối hợp với Sở Khoa học Công nghệ, Sở Tài chính tham mưu Chủ tịch UBND tỉnh xây dựng dự án Trung tâm SOC của tỉnh, kết nối và chia sẻ thông tin, dữ liệu về Trung tâm Giám sát an toàn không gian mạng quốc gia (Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao).

- Thực hiện phối hợp với các sở, ban, ngành và các đơn vị trực thuộc; UBND các xã, phường tham mưu UBND tỉnh ban hành quy chế bảo vệ dữ liệu cá nhân, thông tin quan trọng.

- Chỉ đạo Đội ứng cứu sự cố an ninh mạng của tỉnh xây dựng các tình huống giả định và phương án bảo vệ an toàn, an ninh mạng, tổ chức diễn tập thường xuyên, định kỳ hàng năm theo hướng dẫn của Bộ Công an hoặc khi có yêu cầu.

- Hướng dẫn các biện pháp kỹ thuật cần thiết cho các cơ quan, doanh

nghiệp cung cấp dịch vụ viễn thông, internet và nội dung thông tin mạng, các phương tiện điện tử, thiết bị di động đầu cuối để thực hiện nhiệm vụ đảm bảo an toàn thông tin mạng.

- Ký kết ít nhất 01 quy chế phối hợp giữa các các Sở, ban, ngành, UBND các phường, xã, các doanh nghiệp viễn thông, các trường Đại học trong lĩnh vực đảm bảo an toàn, an ninh thông tin mạng.

2. Sở khoa học và Công nghệ

- Tổ chức triển khai, xây dựng, quản lý, vận hành hạ tầng mạng, trung tâm dữ liệu, hạ tầng, nền tảng, cơ sở dữ liệu dùng chung, phục vụ chuyển đổi số, ứng dụng công nghệ thông tin; phối hợp Công an tỉnh trong thực hiện công tác đảm bảo an ninh mạng đối với hệ thống thông tin tập trung, dùng chung của tỉnh.

- Cử cán bộ có trình độ, kinh nghiệm tham gia xử lý, ứng cứu các sự cố về an toàn thông tin, an ninh mạng xảy ra trên địa bàn tỉnh Đồng Nai khi có yêu cầu của đơn vị điều phối.

- Phối hợp với Công an tỉnh trong công tác giám sát an ninh mạng đối với hệ thống thông tin tại Trung tâm tích hợp dữ liệu; kịp thời trao đổi Công an tỉnh thông tin liên quan đến các sự cố gây mất an ninh mạng đối với hệ thống thông tin tập trung, dùng chung của tỉnh.

- Phối hợp các cơ quan, đơn vị, địa phương triển khai thực hiện hiệu quả công tác tuyên truyền, phổ biến pháp luật về an toàn thông tin, an ninh mạng.

- Rà soát hiện trạng hệ thống thông tin của các Sở, ban, ngành, UBND các phường, xã; tham mưu UBND tỉnh tăng cường đầu tư, nâng cấp hạ tầng công nghệ thông tin đảm bảo đồng bộ, có tính liên thông với các hệ thống giám sát đảm bảo an ninh mạng của tỉnh.

3. Sở Tài chính

- Trên cơ sở chủ trương thực hiện nhiệm vụ được phê duyệt, Sở Tài chính tham mưu Ủy ban nhân dân tỉnh nguồn kinh phí thực hiện theo quy định.

- Thực hiện việc rà soát, kiểm tra, hướng dẫn thực hiện nhiệm vụ, dự án hoặc các chương trình, kế hoạch hàng năm của tỉnh về công tác bảo đảm an ninh mạng có sử dụng nguồn đầu tư công theo đúng quy định pháp luật hiện hành.

4. Các Sở, ban, ngành và các đơn vị trực thuộc; UBND xã, phường

- Phân công lãnh đạo phụ trách, thành lập hoặc chỉ định bộ phận đầu mối chịu trách nhiệm về công tác đảm bảo an ninh mạng tại cơ quan, đơn vị, địa phương theo thẩm quyền quản lý.

- Thực hiện bố trí cán bộ, công chức, viên chức về công tác đảm bảo an ninh mạng tại cơ quan, đơn vị, địa phương mình; kịp thời thông báo về Công an tỉnh khi có sự thay đổi về công tác đảm bảo an ninh mạng tại cơ quan, đơn vị hoặc đang là thành viên tham gia Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh.

- Thực hiện rà soát, đánh giá, xác định cấp độ, lập hồ sơ đề xuất cấp độ an toàn hệ thống thông tin theo quy định tại Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ và Thông tư số 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông và triển khai đầy đủ các phương án đảm bảo an ninh mạng tại cơ quan, đơn vị.

- Định kỳ hàng năm (trước 10/12) hoặc đột xuất báo cáo tình hình thực hiện công tác bảo đảm an ninh mạng tại cơ quan, đơn vị, địa phương về Công an tỉnh để tổng hợp báo cáo các cơ quan cấp trên theo quy định.

- Cử cán bộ tham gia các chương trình huấn luyện, diễn tập và khóa đào tạo, tập huấn về ứng cứu sự cố, bảo đảm an ninh mạng để nâng cao kỹ năng và công tác tham mưu, triển khai giám sát, bảo đảm an ninh mạng.

- Triển khai tổ chức tuyên truyền, phổ biến các văn bản quy phạm pháp luật, tài liệu hướng dẫn chuyên môn, các hoạt động liên quan đến đảm bảo an ninh mạng trên Trang thông tin điện tử, các phương tiện thông tin đại chúng.

- Tích cực phối hợp với cơ quan, đơn vị chủ trì thực hiện các nhiệm vụ được giao theo Kế hoạch này.

5. Các doanh nghiệp viễn thông, Internet hoạt động trên địa bàn tỉnh

Thiết lập, kiện toàn đầu mối đơn vị chuyên trách an ninh mạng trực thuộc để bảo vệ hệ thống, khách hàng của mình; tham gia hỗ trợ các cơ quan, đơn vị nhà nước giám sát, bảo vệ, kiểm tra, đánh giá an ninh mạng dưới sự điều phối của Công an tỉnh; thực hiện nghiêm túc các quy định của pháp luật về cung cấp dịch vụ viễn thông, internet trên địa bàn tỉnh.

6. Trong quá trình thực hiện nếu có khó khăn, vướng mắc, đề nghị các đơn vị, địa phương kịp thời báo cáo Ủy ban nhân dân tỉnh (qua Công an tỉnh) để phối hợp, xử lý. Giao Công an tỉnh chủ trì, giúp Chủ tịch UBND tỉnh theo dõi, hướng dẫn, kiểm tra đôn đốc việc thực hiện và tổng hợp báo cáo theo quy định./.

Nơi nhận:
- Bộ Công an (Cục A05);
- CT, các PCT UBND tỉnh;
- Các sở, ban, ngành, và các đơn vị trực thuộc;
- UBND các xã, phường;
- Các doanh nghiệp cung cấp dịch vụ viễn thông, internet trên địa bàn tỉnh (giao Sở KHCN gửi);
- Chánh, PCVP UBND tỉnh;
- Lưu: VT, KGVX, NC.

TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH

Nguyễn Văn Út