

**CHƯƠNG TRÌNH HÀNH ĐỘNG**

**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 trên địa bàn tỉnh Đồng Nai**

----

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 (sau đây gọi tắt là *Chỉ thị số 57-CT/TW*); Ban Thường vụ Tỉnh ủy xây dựng Chương trình hành động triển khai thực hiện, nội dung cụ thể như sau:

**I. MỤC ĐÍCH, YÊU CẦU**

1. Quán triệt, triển khai thực hiện Chỉ thị số 57-CT/TW, tạo sự thống nhất cao trong nhận thức và hành động của cán bộ, đảng viên và nhân dân, coi đây là nhiệm vụ trọng tâm, thường xuyên trong công tác bảo đảm an ninh quốc gia, giữ gìn trật tự an toàn xã hội, góp phần quản lý hiệu quả, an toàn phục vụ phát triển kinh tế - xã hội của địa phương.

2. Cụ thể hóa và tổ chức thực hiện có hiệu quả các quan điểm, mục tiêu, nhiệm vụ nêu tại Chỉ thị số 57-CT/TW gắn với thực hiện Nghị quyết Đại hội Đảng bộ tỉnh Đồng Nai lần thứ I, nhiệm kỳ 2025 - 2030 và Nghị quyết Đại hội Đảng toàn quốc lần thứ XIV. Tăng cường sự lãnh đạo của các cấp ủy, tổ chức đảng, nâng cao nhận thức, trách nhiệm của cả hệ thống chính trị và toàn dân về an ninh mạng, bảo mật thông tin, an ninh dữ liệu; chủ động sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng.

3. Đề ra các nhiệm vụ cần triển khai thực hiện trong thời gian tới, xác định rõ các công việc, phân công trách nhiệm thực hiện cụ thể; kịp thời đề xuất các giải pháp tháo gỡ khó khăn, vướng mắc phát sinh trong quá trình thực hiện.

**II. MỤC TIÊU**

1. Về Trung tâm giám sát, điều hành an ninh mạng: Hoàn thành xây dựng giai đoạn 1 (**Trong năm 2026**); 100% hệ thống thông tin của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh được bảo vệ theo mô hình 4 lớp và được giám sát an toàn thông tin 24/7/365.

2. Về hạ tầng dữ liệu: 100% dữ liệu dùng chung, dữ liệu chuyên ngành của tỉnh được lưu trữ tập trung tại Trung tâm dữ liệu tỉnh đạt chuẩn an ninh mạng; chấm

dứt tình trạng máy chủ phân tán, không bảo đảm an toàn tại các đơn vị cấp cơ sở.

**3. Về nguồn lực tài chính:** Trên cơ sở đề xuất của cơ quan chức năng và các đơn vị liên quan, căn cứ tiêu chuẩn định mức, chi ngân sách hiện hành và khả năng cân đối của ngân sách địa phương, UBND tỉnh tham mưu bố trí nguồn kinh phí ngân sách nhà nước theo phân cấp cho công tác an ninh mạng và các dự án an ninh mạng theo quy định của Luật ngân sách nhà nước, Luật Đầu tư công và các văn bản pháp luật có liên quan.

**4. Về nguồn nhân lực:** Xây dựng đội ngũ chuyên gia an ninh mạng của tỉnh đủ năng lực làm chủ công nghệ; 100% cán bộ chuyên trách công nghệ thông tin tại các sở, ban, ngành, xã, phường được đào tạo, bồi dưỡng chuyên sâu về an ninh mạng.

**5. Về nhận thức xã hội:** Triển khai sâu rộng phong trào “Bình dân học vụ số”; phân đầu 100% cán bộ, đảng viên và 80% người dân sử dụng thiết bị thông minh được trang bị kỹ năng cơ bản về an toàn thông tin, nhận diện và phòng chống lừa đảo trực tuyến.

### III. NHIỆM VỤ, GIẢI PHÁP

**1. Tăng cường sự lãnh đạo của Đảng, nâng cao nhận thức, trách nhiệm của cả hệ thống chính trị và toàn dân về an ninh mạng, bảo mật thông tin, an ninh dữ liệu**

- Tăng cường sự lãnh đạo, chỉ đạo của các cấp ủy đảng, đẩy mạnh công tác tuyên truyền, thống nhất nhận thức các cơ quan Đảng, Nhà nước về bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là nhiệm vụ trọng yếu, thường xuyên, cấp bách; là trách nhiệm của cả hệ thống chính trị và nhân dân.

- Các cấp ủy, tổ chức đảng, cán bộ, đảng viên cần đổi mới tư duy, nâng cao nhận thức, gắn trách nhiệm người đứng đầu trong triển khai thực hiện nhiệm vụ, phải trực tiếp phụ trách, chỉ đạo rà soát, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo; cán bộ, đảng viên phải gương mẫu thực hiện nghiêm túc, hiệu quả công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu. Công an tỉnh, Bộ Chỉ huy quân sự tỉnh, Văn phòng Tỉnh ủy đóng vai trò nòng cốt.

- Phát huy sự tham gia có hiệu quả của quần chúng nhân dân trong công tác bảo đảm an toàn, an ninh mạng và chủ động ứng phó với các nguy cơ, thách thức từ không gian mạng. Hình thành thế trận An ninh nhân dân trên không gian mạng kết hợp chặt chẽ với thế trận Quốc phòng toàn dân trên không gian mạng. Xây dựng cơ chế hợp tác giữa các cơ quan Đảng, Nhà nước và các doanh nghiệp, hiệp hội doanh nghiệp trên địa bàn tỉnh trong xây dựng và thực thi các chính sách về an toàn, an ninh mạng.

- Chuyển dịch tư duy chiến lược từ “Phòng thủ bị động” sang “Phòng thủ chủ động”, “Phòng thủ tích cực”, xây dựng “Thế trận an ninh mạng chủ động, toàn diện”;

những nguy cơ, thách thức về an ninh mạng, bảo mật thông tin, an ninh dữ liệu phải được nhận diện và xử lý từ sớm, từ xa, sẵn sàng có các biện pháp phòng vệ tương xứng để răn đe, vô hiệu hóa các nguy cơ, bảo vệ lợi ích quốc gia - dân tộc.

- Quán triệt phương châm “Tự chủ, tự lực, tự cường” trong xây dựng tiềm lực an ninh mạng. Tập trung phát triển, khai thác, sử dụng hệ sinh thái sản phẩm, dịch vụ an ninh mạng Việt Nam, ưu tiên làm chủ công nghệ lõi, giải pháp bảo mật tiên tiến, ứng dụng mạnh mẽ trí tuệ nhân tạo, công nghệ mới vào lĩnh vực an ninh mạng, coi đây là những nhiệm vụ chiến lược để bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng. Áp dụng cơ chế đột phá, đặc thù, ưu đãi nhất là trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo để phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng, an ninh dữ liệu.

- 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. Hệ thống chưa bảo đảm an toàn, an ninh thì kiên quyết chưa đưa vào sử dụng. Thường xuyên rà soát, kiểm tra, đánh giá an ninh mạng đối với các hệ thống công nghệ thông tin. Việc thu thập, quản lý, khai thác dữ liệu số phải được bảo vệ ở mức độ cao nhất; tuyệt đối không để lộ, lọt bí mật nhà nước, dữ liệu nhạy cảm, kể cả trong quá trình thử nghiệm.

- Người đứng đầu cấp uỷ, chính quyền, cơ quan, đơn vị chịu trách nhiệm trực tiếp, toàn diện về công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước tại đơn vị mình. Kết quả công tác này là một trong những tiêu chí quan trọng để đánh giá, xếp loại tổ chức, cán bộ, đảng viên, công chức, viên chức và người lao động hằng năm.

- Đổi mới mạnh mẽ nội dung, hình thức tuyên truyền, giáo dục kiến thức, kỹ năng an ninh mạng. Triển khai đánh giá tín nhiệm mạng, phát triển cơ chế liên kết và hợp tác nhằm xây dựng một không gian mạng an toàn, tin cậy, thúc đẩy các giá trị nhân văn và nâng cao ý thức trách nhiệm bảo đảm an ninh không gian mạng đến mọi người dùng; phát động phong trào toàn dân bảo vệ an ninh mạng; phát huy trách nhiệm xã hội của cơ quan báo chí và người có uy tín trong việc định hướng dư luận, lan toả thông tin tích cực và đấu tranh với các thông tin xấu, độc. Tập trung đào tạo, nâng cao năng lực, kỹ năng của lực lượng chuyên trách về an ninh mạng trên địa bàn tỉnh.

- Triển khai hệ thống định danh và xác thực không gian mạng quốc gia; thống nhất định danh công dân, người dùng mạng xã hội, thuê bao viễn thông và tài nguyên Internet (*tên miền, địa chỉ IP...*). Kiên quyết xử lý triệt để tình trạng SIM “rác”, tài khoản “ảo”, nặc danh; áp dụng biện pháp xác thực danh tính bắt buộc đối với người dùng mạng xã hội và cơ chế kiểm soát độ tuổi để bảo vệ trẻ em trên không gian mạng.

## **2. Hoàn thiện thể chế, chính sách và nâng cao hiệu lực, hiệu quả quản lý nhà nước**

- Căn cứ tình hình thực tế tại địa bàn tỉnh Đồng Nai đề rà soát, đề xuất xây dựng, sửa đổi, bổ sung văn bản về bảo đảm an toàn, an ninh mạng cho giao dịch điện tử, chuyển đổi số, hạ tầng số, nền tảng số, bảo vệ thông tin cá nhân trên mạng bảo đảm phù hợp với các văn bản quy phạm pháp luật hiện hành về an toàn, an ninh mạng.

- Thống nhất đầu mối, trách nhiệm quản lý nhà nước bảo đảm hiệu lực, hiệu quả. Trong đó:

*Về an ninh mạng:* Công an tỉnh chịu trách nhiệm trước Ban Thường vụ Tỉnh ủy chủ trì quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với các hệ thống thông tin, cơ sở dữ liệu của toàn hệ thống chính trị trên địa bàn tỉnh và quản lý hoạt động cung cấp sản phẩm, dịch vụ an ninh mạng đối với các hệ thống này (*trừ hệ thống thông tin, cơ sở dữ liệu quân sự và cơ yếu trong phạm vi Bộ Chỉ huy quân sự tỉnh quản lý*).

*Về mật mã và sản phẩm mật mã:* Công an tỉnh, Bộ Chỉ huy quân sự tỉnh, Văn phòng Tỉnh ủy thực hiện trách nhiệm, phạm vi quản lý theo đúng quy định tại Luật An ninh mạng năm 2025.

- Thực hiện nghiêm quy định pháp luật yêu cầu hồ sơ thiết kế hệ thống thông tin, các dự án chuyển đổi số trên địa bàn tỉnh phải có cấu phần an ninh mạng được thẩm định, phê duyệt trước khi đầu tư xây dựng.

- Áp dụng có hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia nhằm tăng tính chủ động phân bổ nguồn lực và giảm thiểu tổn thất. Có cơ chế phối hợp trao đổi, chia sẻ thông tin và quy trình phối hợp ứng cứu sự cố giữa các cơ quan, tổ chức trên địa bàn tỉnh.

- Quy định rõ trách nhiệm của các doanh nghiệp viễn thông, Internet, tài chính, ngân hàng trên địa bàn tỉnh Đồng Nai trong việc bảo đảm an ninh hệ thống và phối hợp với cơ quan chức năng (*Công an tỉnh, Bộ Chỉ huy quân sự tỉnh*) thiết lập cơ chế kết nối kỹ thuật, cung cấp dữ liệu, chứng cứ điện tử nhanh chóng, kịp thời, bảo đảm “đúng, đủ, sạch, sống” để phục vụ công tác điều tra, xử lý tội phạm và bảo vệ chủ quyền quốc gia; đơn giản hóa thủ tục hành chính trong các tình huống khẩn cấp về an ninh mạng.

## **3. Tập trung đầu tư, hiện đại hóa hạ tầng, công nghệ và các giải pháp kỹ thuật bảo đảm an ninh mạng**

- Nâng cao trách nhiệm tự bảo vệ hệ thống thông tin thuộc phạm vi quản lý. Gắn trách nhiệm của người đứng đầu cơ quan chủ quản hệ thống thông tin với trách nhiệm bảo đảm an toàn, an ninh mạng. Xây dựng, cập nhật, vận hành hệ thống thông

tin theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh mạng. Rà soát, lập hồ sơ đề nghị đưa các hệ thống thông tin trọng yếu, phù hợp với quy định của pháp luật vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia (*nếu có*).

- Thực hiện nghiêm túc các quy định pháp luật về bảo vệ an ninh mạng; xác định cấp độ và trách nhiệm bảo đảm an toàn hệ thống thông tin theo từng cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng; nhất là hệ thống thông tin của các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin. Chủ động giám sát, kịp thời phát hiện nguy cơ mất an toàn, an ninh mạng trong quá trình thi công, lắp đặt thiết bị trong các hệ thống thông tin. Ưu tiên sử dụng sản phẩm, giải pháp an toàn, an ninh mạng “Make in Viet Nam”. Khuyến khích xã hội hóa đối với công tác phát triển, ứng dụng sản phẩm mật mã dân sự để bảo mật thông tin.

- Đầu tư nguồn lực, thường xuyên nâng cấp hệ thống, cập nhật bản quyền, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng cho cán bộ, đảng viên và người lao động. Hằng năm tổ chức diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn, an ninh mạng. Sử dụng các giải pháp dùng mật mã để bảo vệ thông tin trong hệ thống thông tin của đơn vị theo quy định.

- Nâng cao năng lực của Trung tâm giám sát, điều hành An ninh mạng tỉnh Đồng Nai thuộc Công an tỉnh. Mở rộng kết nối giám sát an ninh mạng đến toàn bộ cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành, hệ thống thông tin, hệ thống dùng chung của toàn hệ thống chính trị trên địa bàn tỉnh. Đôn đốc các cơ quan, đơn vị, địa phương thiết lập kênh kết nối trao đổi thông tin, dữ liệu phục vụ giám sát, điều phối ứng cứu, khắc phục sự cố an ninh mạng theo hướng dẫn của lực lượng chuyên trách.

- Tổ chức rà soát, kiểm tra, đánh giá định kỳ công tác bảo đảm an ninh thông tin, an ninh mạng. Tập trung phát triển giải pháp kỹ thuật bảo đảm tuyệt đối an toàn cho các hệ thống thông tin trọng yếu; tăng cường phối hợp chặt chẽ, hiệp đồng tác chiến giữa các lực lượng chuyên trách trong bảo vệ an ninh mạng trên địa bàn tỉnh Đồng Nai.

- Rà soát, điều chỉnh quy hoạch hạ tầng công nghệ thông tin theo hướng tập trung máy chủ về các trung tâm dữ liệu đạt chuẩn, đủ điều kiện an ninh mạng. Tăng cường bảo đảm an ninh kết nối, duy trì sự ổn định, thông suốt và an toàn của các luồng dữ liệu, kết nối trong mọi tình huống, không để xảy ra bị động, bất ngờ.

- Bảo đảm nguồn lực tài chính bền vững cho công tác an ninh mạng. Thực hiện nghiêm quy định ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng trong nước trong các dự án đầu tư công của tỉnh. Bảo đảm tỷ lệ kinh phí chi cho an ninh mạng, bảo mật thông tin đạt tối thiểu 15% tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số; đầu tư có trọng tâm, trọng điểm, tránh dàn trải, lãng phí.

#### **4. Xây dựng thể trận an ninh nhân dân gắn với thể trận quốc phòng toàn dân trên không gian mạng; phát triển tiềm lực, công nghệ và nguồn nhân lực**

- Xây dựng thể trận an ninh nhân dân gắn với thể trận quốc phòng toàn dân trên không gian mạng vững chắc. Phát huy vai trò nòng cốt của lực lượng vũ trang nhân dân; huy động sức mạnh tổng hợp của các doanh nghiệp công nghệ, viễn thông và các tầng lớp nhân dân. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet phải xác định rõ trách nhiệm là “tuyên đầu” trong bảo vệ an ninh mạng.

- Tập trung nguồn lực xây dựng nền công nghiệp an ninh mạng tự chủ, tự cường. Ưu tiên sử dụng các sản phẩm cốt lõi, nền tảng “Make in VietNam” bao gồm: Giải pháp tường lửa, phòng, chống mã độc, bảo vệ thiết bị đầu cuối, nền tảng điện toán đám mây và hệ điều hành dùng riêng. Xây dựng cơ chế, chính sách hỗ trợ, thu hút doanh nghiệp công nghệ, cộng đồng khởi nghiệp sáng tạo tham gia phát triển hệ sinh thái an ninh mạng trên địa bàn tỉnh.

- Đẩy mạnh đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao. Tăng cường liên kết giữa Nhà nước - Nhà trường - Doanh nghiệp trong đào tạo, huấn luyện thực chiến. Xây dựng mạng lưới chuyên gia an ninh mạng, sẵn sàng huy động nguồn lực xã hội tham gia ứng cứu sự cố, tình huống nguy hiểm về an ninh mạng. Tiếp tục hoàn thiện cơ chế, chính sách thu hút, đãi ngộ nhân tài, chuyên gia giỏi tham gia phục vụ công tác an ninh mạng trên địa bàn tỉnh.

#### **5. Về hợp tác quốc tế trên lĩnh vực an ninh mạng**

Tăng cường phối hợp quốc tế trong phòng, chống và ứng phó sự cố tấn công mạng; điều tra, truy tố tội phạm mạng xuyên quốc gia; bảo đảm độc lập, tự chủ, chủ quyền quốc gia trong quá trình hợp tác, tiếp thu kinh nghiệm, công nghệ và chuẩn mực quốc tế về an ninh mạng; cử cán bộ đi đào tạo, huấn luyện chuyên sâu tại nước ngoài và tích cực tham gia các cuộc diễn tập an ninh mạng quốc tế.

### **IV. TỔ CHỨC THỰC HIỆN**

1. Các ban, ngành và cấp ủy, chính quyền địa phương, đơn vị căn cứ chức năng, nhiệm vụ được giao, tổ chức nghiên cứu, quán triệt, tuyên truyền, xây dựng và ban hành kế hoạch triển khai thực hiện Chỉ thị số 57-CT/TW theo Chương trình hành động của Ban Thường vụ Tỉnh ủy và Phụ lục nhiệm vụ trọng tâm thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh Đồng Nai (*gửi kèm Chương trình hành động này*) chịu trách nhiệm trước Ban Thường vụ Tỉnh ủy về kết quả công tác bảo đảm an ninh mạng tại cơ quan, đơn vị, địa phương mình.

2. Đảng ủy UBND tỉnh chủ trì, phối hợp Đảng ủy Công an tỉnh và các cơ quan liên quan theo dõi, kiểm tra, giám sát, đánh giá kết quả thực hiện, định kỳ báo cáo Ban Thường vụ Tỉnh ủy, Ban Chấp hành Đảng bộ tỉnh.

3. Quá trình tổ chức triển khai thực hiện, Ban Chấp hành Đảng bộ tỉnh, Ban Thường vụ Tỉnh ủy quyết định việc điều chỉnh, bổ sung các nhiệm vụ cụ thể trong Chương trình hành động và Phụ lục để phù hợp với điều kiện tình hình thực tiễn, đáp ứng các yêu cầu nhiệm vụ chính trị của tỉnh./.

Nơi nhận:

- Ban Bí thư Trung ương Đảng,
- Đảng ủy các cơ quan Đảng tỉnh,
- Đảng ủy Ủy ban nhân dân tỉnh,
- Các CQ chuyên trách TMGV Tỉnh ủy,
- Các sở, ban, ngành, UBMTTQVN tỉnh,
- Đảng ủy, UBND các xã, phường,
- Lãnh đạo VPTU,
- Phòng: TH, CDS-CY,
- Lưu VPTU.

**T/M BAN THƯỜNG VỤ  
PHÓ BÍ THƯ THƯỜNG TRỰC**

**Tôn Ngọc Hạnh**

**PHỤ LỤC**  
**NHIỆM VỤ TRỌNG TÂM THỰC HIỆN CÔNG TÁC BẢO ĐẢM AN NINH MẠNG, BẢO MẬT THÔNG TIN,**  
**AN NINH DỮ LIỆU TRONG HỆ THỐNG CHÍNH TRỊ TRÊN ĐỊA BÀN TỈNH ĐỒNG NAI**  
*(Kèm theo Chương trình hành động số -CTr/TU ngày tháng năm 2026 của Ban Thường vụ Tỉnh ủy)*

STT	Tên chương trình, đề án, nhiệm vụ	Cơ quan, tổ chức chủ trì	Cơ quan, tổ chức phối hợp	Thời gian hoàn thành
<b>I. Tăng cường sự lãnh đạo của Đảng, nâng cao nhận thức, trách nhiệm của cả hệ thống chính trị và toàn dân về an ninh mạng, bảo mật thông tin, an ninh dữ liệu</b>				
1	Kiện toàn Tiểu ban An ninh mạng tỉnh Đồng Nai	Đảng ủy Công an tỉnh	Các sở, ban, ngành có liên quan	Quý 1/2026 (đã hoàn thành)
2	Phát huy sự tham gia có hiệu quả của quần chúng nhân dân trong công tác bảo đảm an toàn, an ninh mạng và chủ động ứng phó với các nguy cơ, thách thức từ không gian mạng.	Công an tỉnh	Các sở, ban, ngành địa phương	Thường xuyên
3	Hình thành Thế trận An ninh nhân dân trên không gian mạng kết hợp chặt chẽ với Thế trận Quốc phòng toàn dân trên không gian mạng.	- Công an tỉnh; - Bộ Chỉ huy quân sự tỉnh.	Các sở, ban, ngành địa phương	Thường xuyên
4	Triển khai các quy định về bảo đảm an ninh mạng, an toàn thông tin cho các cơ sở dữ liệu dùng chung, chuyên	Công an tỉnh	Các cơ quan, doanh nghiệp trên địa bàn tỉnh	Thường xuyên

STT	Tên chương trình, đề án, nhiệm vụ	Cơ quan, tổ chức chủ trì	Cơ quan, tổ chức phối hợp	Thời gian hoàn thành
	ngành theo TCVN 11930:2017 và TCVN 14432:2025			
5	Chủ động tự rà soát, kiểm tra, đánh giá an ninh mạng đối với các hệ thống công nghệ thông tin	Các sở, ban, ngành, đoàn thể tỉnh, Đảng ủy, UBND các xã, phường	Công an tỉnh	Thường xuyên
6	Kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin do đơn vị quản lý, vận hành.	Công an tỉnh	Các cơ quan, đơn vị, địa phương trên địa bàn tỉnh	Định kỳ hàng năm kiểm tra, đánh giá đối với hệ thống cấp độ 3; hai năm một lần đối với các hệ thống thông tin cấp độ 1, cấp độ 2. Trong đó, Công an tỉnh chủ trì kiểm tra, đánh giá các hệ thống thông tin cấp độ 2, cấp độ 3; các cơ quan, đơn vị chủ trì triển khai đối với hệ thống trong tổ chức mình.

<b>STT</b>	<b>Tên chương trình, đề án, nhiệm vụ</b>	<b>Cơ quan, tổ chức chủ trì</b>	<b>Cơ quan, tổ chức phối hợp</b>	<b>Thời gian hoàn thành</b>
7	Tổ chức các hoạt động tuyên truyền, phổ biến nâng cao nhận thức của cán bộ, công chức, viên chức và người lao động tại đơn vị, như: hội nghị, sinh hoạt chuyên đề...	Các sở, ban, ngành, đoàn thể tỉnh, Đảng ủy, UBND các xã, phường	Công an tỉnh	Thường xuyên
<b>II. Hoàn thiện thể chế, chính sách và nâng cao hiệu lực, hiệu quả quản lý nhà nước</b>				
8	Rà soát, đề xuất xây dựng, sửa đổi, bổ sung văn bản về bảo đảm an toàn, an ninh mạng cho giao dịch điện tử, chuyển đổi số, hạ tầng số, nền tảng số, bảo vệ thông tin cá nhân trên mạng bảo đảm phù hợp với các văn bản quy phạm pháp luật hiện hành về an toàn, an ninh mạng.	Công an tỉnh	Các sở, ban, ngành có liên quan	Thường xuyên
9	Thực hiện việc xác định cấp độ và phương án bảo đảm an ninh mạng, an toàn thông tin theo cấp độ; hoàn thiện hồ sơ đề xuất cấp độ trình cơ quan có thẩm quyền phê duyệt.	Các sở, ban, ngành, đoàn thể tỉnh, Đảng ủy, UBND các xã, phường	Công an tỉnh	Thường xuyên
<b>III. Tập trung đầu tư, hiện đại hóa hạ tầng, công nghệ và các giải pháp kỹ thuật bảo đảm an ninh mạng</b>				

<b>STT</b>	<b>Tên chương trình, đề án, nhiệm vụ</b>	<b>Cơ quan, tổ chức chủ trì</b>	<b>Cơ quan, tổ chức phối hợp</b>	<b>Thời gian hoàn thành</b>
10	Rà soát, lập hồ sơ đề nghị đưa các hệ thống thông tin trọng yếu, phù hợp với quy định của pháp luật vào Danh mục hệ thống thông tin quan trọng về an ninh quốc gia nếu có.	Các cơ quan, đơn vị, địa phương trên địa bàn tỉnh	Công an tỉnh	Thường xuyên
11	Ưu tiên sử dụng sản phẩm, giải pháp an toàn, an ninh mạng “Make in Viet Nam”.	Các cơ quan, đơn vị, địa phương trên địa bàn tỉnh		Thường xuyên
12	Đầu tư nguồn lực, thường xuyên nâng cấp hệ thống, cập nhật bản quyền, nâng cao nhận thức và kỹ năng an toàn, an ninh mạng cho cán bộ, công chức, viên chức và người lao động.	Các cơ quan, đơn vị, địa phương trên địa bàn tỉnh	Sở Tài chính	Thường xuyên
13	Tổ chức diễn tập thực chiến về an ninh mạng.	Công an tỉnh	Các sở, ban, ngành có liên quan	Năm 2026
14	Xây dựng Trung tâm giám sát, điều hành an ninh mạng tỉnh Đồng Nai	Công an tỉnh	Các sở, ban, ngành có liên quan	Năm 2026
15	Mở rộng kết nối giám sát an ninh mạng đến toàn bộ cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành, hệ thống thông tin, hệ thống dùng chung của toàn hệ thống chính trị trên địa bàn tỉnh.	Công an tỉnh	Các sở, ban, ngành, đoàn thể tỉnh, Đảng ủy, UBND các xã, phường	Năm 2026

<b>STT</b>	<b>Tên chương trình, đề án, nhiệm vụ</b>	<b>Cơ quan, tổ chức chủ trì</b>	<b>Cơ quan, tổ chức phối hợp</b>	<b>Thời gian hoàn thành</b>
16	Bảo đảm tỷ lệ kinh phí chi cho an ninh mạng, bảo mật thông tin đạt tối thiểu 15% tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số; đầu tư có trọng tâm, trọng điểm, tránh dàn trải, lãng phí.	Các sở, ban, ngành, đoàn thể tỉnh, Đảng ủy, UBND các xã, phường	Sở Tài chính	Thường xuyên
<b>IV. Xây dựng thể trận an ninh nhân dân gắn với thể trận quốc phòng toàn dân trên không gian mạng; phát triển tiềm lực, công nghệ và nguồn nhân lực</b>				
17	Huy động sức mạnh tổng hợp của các doanh nghiệp công nghệ, viễn thông và các tầng lớp nhân dân. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet phải xác định rõ trách nhiệm là “tuyên đầu” trong bảo vệ an ninh mạng.	UBND tỉnh	- Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet trên địa bàn tỉnh Đồng Nai; - Công an tỉnh.	Thường xuyên
18	Tổ chức tập huấn cho lực lượng nhân sự có chức năng bảo đảm an toàn, an ninh mạng, công nghệ thông tin tại các sở, ban, ngành, xã, phường về công tác bảo đảm an ninh mạng.	Công an tỉnh	Các sở, ban, ngành, đoàn thể tỉnh, Đảng ủy, UBND các xã, phường	Năm 2026
<b>V. Về hợp tác quốc tế trên lĩnh vực an ninh mạng</b>				
19	Cử cán bộ đi đào tạo, huấn luyện	Sở Nội vụ	Các sở, ban, ngành,	Thường xuyên

<b>STT</b>	<b>Tên chương trình, đề án, nhiệm vụ</b>	<b>Cơ quan, tổ chức chủ trì</b>	<b>Cơ quan, tổ chức phối hợp</b>	<b>Thời gian hoàn thành</b>
	chuyên sâu tại nước ngoài và tích cực tham gia các cuộc diễn tập an ninh mạng trong và ngoài nước.		đoàn thể tỉnh, Đảng ủy, UBND các xã, phường	