TỈNH ỦY QUẢNG NGÃI
BAN CHỈ ĐẠO VỀ PHÁT TRIỂN KHOA HỌC, CÔNG NGHỆ, ĐỔI MỚI SÁNG TẠO VÀ CHUYỂN ĐỔI SỐ
*
Số 02-KH/BCĐ

ĐẢNG CỘNG SẢN VIỆT NAM

Quảng Ngãi, ngày 24 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 tỉnh Quảng Ngãi
---

Thực hiện 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, Ban Chỉ đạo tỉnh về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số ban hành Kế hoạch bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh, như sau:

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.

- Chương trình hành động số 20-CTr/TU ngày 23/4/2026 của Ban Thường vụ Tỉnh ủy về 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.

II. MỤC TIÊU VÀ YÊU CÀU

1. Mục tiêu chung

- Quán triệt, tổ chức triển khai, thực hiện nghiêm túc, có hiệu quả chỉ đạo của Ban Chỉ đạo Trung ương về công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn tỉnh.

- Xây dựng không gian mạng trên địa bàn tỉnh an toàn, lành mạnh, tin cậy; nâng cao năng lực tự chủ, tự cường về an ninh mạng; bảo vệ vững chắc an ninh quốc

gia, trật tự, an toàn xã hội trên không gian mạng; bảo đảm an toàn hệ thống thông tin của các cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội; bảo vệ dữ liệu cá nhân, dữ liệu nội bộ, dữ liệu quan trọng, bí mật nhà nước; phục vụ hiệu quả nhiệm vụ chuyển đổi số, phát triển kinh tế - xã hội, củng cố quốc phòng, an ninh.

2. Mục tiêu cụ thể

2.1. Trong năm 2026

- Về công tác lãnh đạo, chỉ đạo: 100% cấp ủy, tổ chức đảng, cơ quan, đơn vị quán triệt, triển khai nghiêm túc nội dung Kế hoạch này; xác định quan điểm bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là nhiệm vụ trọng yếu, thường xuyên, cấp bách, nhằm tạo chuyển biến mạnh mẽ, nâng cao nhận thức và hành động về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong toàn hệ thống chính trị và xã hội trên địa bàn tỉnh.

- **Về thể chế:** 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 của tỉnh hiện đại, đồng bộ, đủ năng lực bảo vệ chủ quyền không gian mạng: (1) 100% các hệ thống thông tin của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị-xã hội trong tỉnh được rà soát, khắc phục các lỗ hổng, điểm yếu an ninh mạng. (2) 100% 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 hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu)* được kết nối, chia sẻ thông tin, dữ liệu giám sát an ninh mạng 24/7 với Trung tâm An ninh mạng cấp tỉnh và Trung tâm An ninh mạng quốc gia. (3) Bảo đảm hạ tầng mật mã quốc gia hoạt động ổn định, bảo mật phục vụ trao đổi dữ liệu bí mật nhà nước từ cấp tỉnh đến 100% xã, phường và đặc khu. (4) Xây dựng Trung tâm An ninh mạng cấp tỉnh giám sát liên tục 24/7, kết nối, chia sẻ thông tin, điều phối, xử lý sự cố với Trung tâm An ninh mạng quốc gia.

- 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; thường xuyên đào tạo, bồi dưỡng đội ngũ chuyên gia an ninh mạng chất lượng cao; tổ chức ít nhất 01 cuộc diễn tập thực hiện an toàn thông tin mạng cấp tỉnh nhằm nâng cao năng lực chỉ huy, điều hành, phối hợp liên ngành và khả năng ứng phó, khắc phục sự cố an ninh mạng trong tình huống thực tế.

- Quản trị: Tăng cường kỷ luật, kỷ cương trong quản lý nhà nước về an ninh mạng; thực hiện quản trị an ninh mạng dựa trên đánh giá rủi ro, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật.

- 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.

2.2. Đến năm 2030

- Vị thế quốc gia: Tuân thủ, thực hiện nghiêm các quy định về An ninh mạng, 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) của Liên minh Viễn thông Quốc tế (ITU).

- **Thể chế:** Hoàn thiện cơ chế pháp lý 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. 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:** Xây dựng và 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; ban hành quy hoạch hạ tầng công nghệ thông tin tổng thể từ Trung ương đến địa phương.

- **Nhân lực:** Đào tạo và xây dựng được đội ngũ chuyên gia an ninh mạng trình độ cao, đáp ứng nhu cầu.

- **Quản trị:** Các sở, ban, ngành, địa phương trong tỉnh và các tổ chức 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.

- **Công nghệ:** Tỉ trọng sản phẩm, dịch vụ an ninh mạng "Make in Vietnam" chiếm trên 50% thị trường trong tỉnh. Các hệ thống thông tin tại các cơ quan trong hệ thống chính trị trên địa bàn tỉnh ưu tiên sử dụng các sản phẩm, dịch vụ, giải pháp an ninh mạng "Make in Vietnam".

2.3. Tầm nhìn chiến lược đến năm 2045

Xây dựng nền an ninh mạng bền vững, tự chủ, có năng lực cạnh tranh. Hình thành đội ngũ chuyên gia đầu ngành, nhà khoa học công nghệ số trình độ quốc tế; làm chủ các công nghệ cốt lõi, giảm phụ thuộc nhập khẩu. Phát triển hạ tầng an ninh mạng và hạ tầng số hiện đại; xây dựng các trung tâm đổi mới sáng tạo, khu công nghiệp công nghệ cao; doanh nghiệp về ngành công nghiệp an ninh mạng.

3. Yêu cầu

- Kế hoạch phải được quán triệt và triển khai thống nhất trong toàn bộ hệ thống chính trị, tránh dàn trải, cục bộ, thiếu tập trung.

- Nhiệm vụ phải được tổ chức thực hiện với quyết tâm cao, có sản phẩm cụ thể, đo lường được, bảo đảm tiến độ và hiệu quả thực chất.

- Phát huy tối đa tiềm năng, trí tuệ Việt Nam, gắn với tiếp thu, làm chủ và ứng dụng hiệu quả các thành tựu công nghệ, kỹ thuật tiên tiến của thế giới.

- Gắn trách nhiệm người đứng đầu với kết quả bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; coi đây là tiêu chí quan trọng trong đánh giá, quy hoạch, bổ nhiệm cán bộ lãnh đạo, quản lý các cấp.

III. NHIỆM VỤ TRỌNG TÂM NĂM 2026

1. Tổ chức kiện toàn, triển khai hoạt động Đội ứng cứu sự cố an ninh mạng tỉnh. Thành lập Đội ứng cứu sự cố an ninh mạng nội bộ tại các đơn vị chủ quản hệ thống thông tin từ cấp độ 2 trở lên, hình thành mạng lưới ứng cứu sự cố an ninh mạng trên địa bàn tỉnh.

2. Các cơ quan chủ quản các cơ sở dữ liệu, hệ thống thông tin trong hệ thống chính trị có trách nhiệm: (1) Rà soát, khắc phục tổng thể về an ninh mạng, bảo mật thông tin, an ninh dữ liệu đối với hệ thống thông tin theo tiêu chuẩn TCVN 14423: 2025 và nguồn nhân lực thuộc phạm vi quản lý. (2) Triển khai giám sát an ninh mạng tại cơ quan, đơn vị thuộc phạm vi quản lý. (3) Báo cáo định kỳ và đột xuất kết quả, tiến độ và mức độ tuân thủ về cơ quan có thẩm quyền; kiến nghị biện pháp hoàn thiện thể chế, tiêu chuẩn và phân bổ nguồn lực khi cần. (4) Xác định trách nhiệm của người đứng đầu về an ninh mạng.

3. Nâng cao năng lực của giám sát, điều hành an toàn, an ninh mạng tỉnh tiến tới xây dựng Trung tâm An ninh mạng cấp tỉnh phù hợp với điều kiện thực tiễn của tỉnh và hướng dẫn của Bộ Công an; mở rộng kết nối, chia sẻ dữ liệu giám sát, cảnh báo an ninh mạng với các hệ thống thông tin quan trọng 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.

4. Phối hợp xây dựng, vận hành Hệ thống phòng vệ mạng quốc gia nhằm bảo vệ an ninh mạng vòng ngoài cho các hệ thống thông tin, tài nguyên trọng yếu trên Internet của các cơ quan ban, bộ, ngành, địa phương, cơ quan, doanh nghiệp Việt Nam.

5. Ban hành các quy định, tài liệu hướng dẫn về kiểm tra, đánh giá, bảo đảm an ninh mạng, an toàn thông tin cho các cơ sở dữ liệu, hệ thống dùng chung trong

hệ thống chính trị; định kỳ tổ chức kiểm tra, đánh giá việc thực hiện các quy định đảm bảo an ninh mạng, an toàn thông tin theo quy định.

6. Rà soát, trình cấp có thẩm quyền xem xét ban hành hoặc điều chỉnh quy hoạch hạ tầng công nghệ thông tin tổng thể từ cấp tỉnh đến cấp xã theo hướng tập trung, chuẩn hoá trung tâm dữ liệu. Đầu tư, nâng cấp hạ tầng công nghệ thông tin đáp ứng yêu cầu và tuân thủ quy hoạch đã được ban hành.

III. NHIỆM VỤ TRỌNG TÂM ĐẾN NĂM 2030

1. Nâng cao nhận thức cho toàn hệ thống chính trị và người dân

- Tiếp tục đẩy mạnh triển khai các chương trình đào tạo, bồi dưỡng, phổ biến kiến thức an ninh mạng trên nền tảng "Bình dân học vụ số".

- 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.

- 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.

- Triển khai các giải pháp định danh và 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.

- 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. Hoàn thiện thể chế, khung pháp lý

- Tiếp tục rà soát, đề xuất 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.

- Phối hợp 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.

- Phối hợp xây dựng Khung quản trị rủi ro an ninh mạng quốc gia và chỉ số đánh giá năng lực bảo đảm an ninh mạng.

- Phối hợp hoàn thiện các cơ chế trao đổi, chia sẻ thông tin trong nước và quốc tế về an ninh mạng.

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

- Phối hợp triển khai kiến trúc bảo vệ an ninh mạng quốc gia đa lớp hỗ trợ bảo

vệ cho toàn bộ hạ tầng mạng Internet và các hệ thống thông tin của tỉnh.

- Quy hoạch và triển khai đồng bộ các nhóm giải pháp: (1) Bảo vệ hạ tầng mạng. (2) Bảo vệ thiết bị đầu cuối. (3) Bảo vệ ứng dụng, dịch vụ. (4) Bảo vệ dữ liệu. (5) Bảo vệ người dùng.

- Khuyến khích xã hội hoá nghiên cứu, phát triển và ứng dụng mật mã dân sự phục vụ bảo mật thông tin.

- Bảo vệ tuyệt đối an toàn các hệ thống thông tin quan trọng, các cơ sở dữ liệu quốc gia về dân cư, đất đai, tài chính, y tế, giáo dục, bảo hiểm, tư pháp... khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin. Kết nối, chia sẻ dữ liệu liên thông trên nguyên tắc bảo mật, an toàn, đúng pháp luật, khắc phục tình trạng cát cứ, phân mảnh dữ liệu.

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

- Phối hợp xây dựng thị trường cạnh tranh lành mạnh, minh bạch; hình thành các trung tâm nghiên cứu, vườn ươm hỗ trợ khởi nghiệp và không gian đổi mới sáng tạo để hỗ trợ doanh nghiệp, nhất là các doanh nghiệp khởi nghiệp sáng tạo, thúc đẩy gắn kết giữa nghiên cứu - triển khai - thương mại hoá sản phẩm.

- Ưu tiên sử dụng các sản phẩm, giải pháp nội địa đáp ứng được các tiêu chuẩn, quy chuẩn trong các dự án, hệ thống trọng yếu nhằm vừa tạo thị trường, vừa thúc đẩy và hỗ trợ doanh nghiệp Việt Nam phát triển. Phù hợp chủ trương nâng cao khả năng tự chủ chiến lược của đất nước.

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 đề xuất 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

- Tiếp tục hoàn thiện cơ chế, chính sách thu hút, đãi ngộ chuyên gia tham gia phục vụ công tác an ninh mạng.

- 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.

- 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 tham gia hỗ trợ công tác bảo đảm an ninh mạng.

- Tăng cường nhân lực bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho tỉnh theo quy định.

7. Hợp tác quốc tế trên lĩnh vực an ninh mạng

- Phối hợp tham gia xây dựng các khuôn khổ pháp lý, chuẩn mực chung của quốc tế.

- Phối hợp đưa Công ước Hà Nội về chống tội phạm mạng 2025 có hiệu lực và thúc đẩy việc thực hiện hiệu quả, thực chất Công ước.

- Tăng cường hợp tác chia sẻ thông tin, điều tra tội phạm mạng xuyên quốc gia; tham gia diễn tập quốc tế.

IV. TỔ CHỨC THỰC HIỆN

1. Phân công trách nhiệm

1.1. Ban Chỉ đạo tỉnh

Chịu trách nhiệm chỉ đạo toàn diện việc triển khai Kế hoạch; trực tiếp cho ý kiến chỉ đạo về các chủ trương, cơ chế, chính sách lớn; chỉ đạo tháo gỡ kịp thời các khó khăn, vướng mắc mang tính liên ngành, các điểm nghẽn vượt thẩm quyền của các sở, ban, ngành, địa phương.

1.2. Thường trực Ban Chỉ đạo

Chịu trách nhiệm chỉ đạo, điều hành trực tiếp, thường xuyên quá trình tổ chức thực hiện Kế hoạch; tổ chức giao ban định kỳ với Cơ quan Thường trực Tiểu ban An ninh mạng tỉnh và các cơ quan liên quan trong việc hướng dẫn, đôn đốc, kiểm tra, giám sát tiến độ, tháo gỡ khó khăn, vướng mắc, bảo đảm Kế hoạch được triển khai đồng bộ, thống nhất, hiệu quả trong hệ thống chính trị.

1.3. Ban Tuyên giáo và Dân vận Tỉnh 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. **Nhiệm vụ thường xuyên.**

1.4. Đảng ủy Ủy ban nhân dân tỉnh

Lãnh đạo Ủy ban nhân dân tỉnh chỉ đạo các cơ quan, đơn vị liên quan triển khai thực hiện các nhiệm vụ:

- Thực hiện kết nối, liên thông, chia sẻ dữ liệu giữa các hệ thống thông tin phục vụ hoạt động và chỉ đạo, điều hành của các cơ quan trong hệ thống chính trị trong tỉnh (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 và bảo mật thông tin. **Hoàn thành trong tháng 4/2026.**

- Rà soát, trình cấp có thẩm quyền xem xét, điều chỉnh quy hoạch hạ tầng thông tin tổng thể từ cấp tỉnh 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 theo quy định. **Theo lộ trình triển khai của Bộ Khoa học và Công nghệ**.

- 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; 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"; triển khai "Khung Năng lực số và An toàn mạng 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). **Nhiệm vụ thường xuyên, theo hướng dẫn và lộ trình triển khai của Bộ Giáo dục và Đào tạo**.

- Rà soát, cân đối ngân sách, bố trí đầy đủ kinh phí cho các cơ quan liên quan để triển khai thực hiện các nhiệm vụ về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu tại các cơ quan, đơn vị, địa phương trong tỉnh. **Nhiệm vụ thường xuyên**.

- Theo chức năng, nhiệm vụ chủ động tham mưu, phối hợp thực hiện các nội dung công tác theo Kế hoạch này. **Nhiệm vụ thường xuyên**.

1.5. Đảng uỷ Công an tỉnh

Lãnh đạo, chỉ đạo Công an tỉnh chịu trách nhiệm trước Ủy ban nhân dân tỉnh thực hiện thống nhất công tác quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu trên địa bàn tỉnh *(trừ lĩnh vực quân sự, quốc phòng và cơ yếu)*, cụ thể như sau:

- Giữ vai trò cơ quan thường trực về vấn đề bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

- 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. **Hoàn thành trước tháng 3/2027.**

- Tham mưu chỉ đạo huy động mọi nguồn lực để khắc phục những lỗ hổng bảo mật trong các hệ thống thông tin. **Hoàn thành trong tháng 4/2026.**

- Phối hợp với các cơ quan để tổ chức thẩm định, phê duyệt cấp độ 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.**

- Chủ trì, phối hợp tham mưu tổ chức rà soát, đánh giá tổng thể an ninh mạng, bảo mật thông tin và an ninh dữ liệu đối với hệ thống thông tin và nguồn nhân lực. **Hoàn thành trong tháng 6/2026.**

- Triển khai mô hình bảo đảm an toàn thông tin "04 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 khác quan và minh bạch. [4] Kết nối, chia sẻ thông tin với hệ thống giám sát an ninh mạng quốc gia, bảo đảm sự phối hợp liên thông trên phạm vi toàn quốc (trừ các hệ thống thông tin quân sự, quốc phòng, cơ yếu). **Hoàn thành trong tháng 4/2026.**

- Chủ trì, phối hợp với các sở, ban, ngành tham mưu UBND tỉnh phối hợp xây dựng, triển khai các quy định, quy trình, quy chế tạo hành lang pháp lý phục vụ công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu hệ thống chính trị nêu tại Kế hoạch này.

- Chủ trì, phối hợp với Sở Giáo dục và Đào tạo và 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. (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.**

- Phối hợp 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.**

- Triển khai hiệu quả, có thực chất Công ước Hà Nội về chống tội phạm mạng năm 2025. **Nhiệm vụ thường xuyên.**

1.6. Đảng ủy Quân sự tỉnh

Lãnh đạo, chỉ đạo Bộ Chỉ huy Quân sự tỉnh chịu trách nhiệm toàn diện trước Ủy ban nhân dân tỉnh 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, cụ thể:

- 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. **Nhiệm vụ thường xuyên.**

- 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 thuộc phạm vi quản lý (bao gồm cả hệ thông 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). **Nhiệm vụ thường xuyên.**

- Theo chức năng, nhiệm vụ chủ động tham mưu, phối hợp thực hiện các nội dung công tác theo Kế hoạch này. **Nhiệm vụ thường xuyên.**

1.7. Đảng ủy Hội đồng nhân dân tỉnh

Lãnh đạo, chỉ đạo rà soát, sửa đổi, bổ sung kịp thời ban hành các văn bản quy phạm pháp luật, văn bản hướng dẫn; tổ chức triển khai thực hiện các nhiệm vụ được giao và chủ động hướng dẫn, xử lý các vấn đề phát sinh theo chức năng, nhiệm vụ, thẩm quyền và lĩnh vực quản lý. **Nhiệm vụ thường xuyên.**

1.8. Người đứng đầu các cơ quan, tổ chức trong hệ thống chính trị từ cấp tỉnh đến cấp xã

- 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, mất 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 dầu, để phục vụ công tác xếp loại hằng năm.

- Ủy ban nhân dân các xã, phường, đặc khu chủ động thực hiện rà soát, cân đối, bố trí kinh phí theo thẩm quyền để triển khai các nhiệm vụ về công tác chuyển đổi số, an ninh mạng, bảo mật thông tin, an ninh dữ liệu tại các cơ quan, đơn vị ở địa phương.

1.9. Văn phòng Tỉnh ủy – Cơ quan Thường trực Ban Chỉ đạo

Thường xuyên theo dõi, tổng hợp, đánh giá kết quả việc thực hiện Kế hoạch này và cập nhật thông tin, số liệu báo cáo lên hệ thống theo dõi tình hình, thực hiện các nghị quyết, chỉ thị, kết luận của Trung ương (https://theodoinq.vn) theo quy định.

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.

- 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 thực hiện cập nhật báo cáo định kỳ hằng tháng hoặc đột xuất (nếu có) trên Hệ thống theo dõi tình hình, thực hiện các nghị quyết, chỉ thị, kết luận của Trung ương (tại địa chỉ: https://theodoinq.dcs.vn).

Các cấp ủy, tổ chức đảng, các cơ quan, đơn vị triển khai thực hiện nghiêm túc Kế hoạch này.

Nơi nhận:
- VPTW Đảng – Cơ quan Thường trực BCĐTW về phát triển KHCN, ĐMST và CĐS,
- Các cơ quan chuyên trách TM,GV Tỉnh uỷ,
- Các đảng ủy trực thuộc Tỉnh ủy,
- Đảng uỷ các xã, phường, đặc khu,
- Các sở, ban, ngành tỉnh,
- Các đơn vị sự nghiệp trực thuộc: Tỉnh ủy, UBND tỉnh,
- Thành viên Ban Chỉ đạo của tỉnh,
- VPTU: CVP, PCVP Tỉnh ủy, các phòng chuyên môn,
- Lưu Văn phòng Tỉnh uỷ.

PHÓ BÍ THƯ
kiêm
PHÓ TRƯỞNG BAN

TỈNH ỦY QUẢNG NGÃI

U Huấn