TỈNH ỦY KHÁNH HÒA
BAN CHỈ ĐẠO
VỀ PHÁT TRIỂN KHOA HỌC, CÔNG NGHỆ, ĐỔI MỚI SÁNG TẠO VÀ CHUYỂN ĐỔI SỐ TỈNH
*

Số 07-KH/BCĐ

ĐẢNG CỘNG SẢN VIỆT NAM

Khánh Hòa, ngày 16 tháng 3 năm 2026

KẾ HOẠCH

Bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị tỉnh Khánh Hoà

Căn cứ 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;

Căn cứ 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;

Căn cứ Kế hoạch số 04-KH/BCĐTW, ngày 05/01/2026 của Ban Chỉ đạo Trung ương về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị;

Căn cứ Nghị quyết số 48-NQ/TU, ngày 20/02/2025 của Ban Chấp hành Đảng bộ tỉnh thực hiện 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;

Căn cứ Quyết định số 172-QĐ/TU, ngày 12/12/2025 của Tỉnh ủy Khánh Hòa về kiện toàn Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số tỉnh Khánh Hòa;

Căn cứ Quyết định số 1614b-QĐ/TU, ngày 14/02/2025 quy định về chức năng, nhiệm vụ, quyền hạn, chế độ làm việc, quan hệ công tác của Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số tỉnh Khánh Hòa.

Căn cứ Thông báo số 03-TB/BCĐ, ngày 16/12/2025 của Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số tỉnh Khánh Hòa phân công nhiệm vụ các thành viên Ban Chỉ đạo.

Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số tỉnh Khánh Hòa (sau đây gọi tắt là Ban Chỉ đạo) ban hành Kế hoạch bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị tỉnh Khánh Hoà cụ thể như sau:

I. MỤC TIÊU VÀ YÊU CẦU

1. Mục tiêu chung: Xây dựng không gian mạng tỉnh Khánh Hòa vững mạnh, có năng lực phản ứng nhanh với mọi sự cố mất an toàn thông tin. Phấn đấu đưa Khánh Hòa vào nhóm các tỉnh dẫn đầu về chỉ số an toàn, an ninh mạng, góp phần bảo đảm môi trường số ổn định cho công cuộc chuyển đổi số toàn diện, phát triển kinh tế-xã hội, bảo đảm quốc phòng-an ninh, xây dựng Đảng và hệ thống chính trị vững mạnh.

2. Mục tiêu cụ thể

a) Mục tiêu năm 2026

- **Về công tác lãnh đạo, chỉ đạo:** Chuyển đổi từ nhận thức sang hành động quyết liệt. Người đứng đầu cấp ủy, chính quyền và thủ trưởng các cơ quan, ban ngành trực tiếp lãnh đạo, chỉ đạo công tác đảm bảo an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

Lãnh đạo, chỉ đạo triển khai các chiến dịch truyền thông đảm bảo người dân nắm được những kỹ năng cơ bản về phòng chống lừa đảo trực tuyến thông qua vai trò nòng cốt của Tổ công nghệ số cộng đồng.

- Về thể chế: xây dựng cơ chế, chính sách thu hút đầu tư nhằm khuyến khích, tạo thuận lợi cho doanh nghiệp công nghệ số, an ninh mạng đầu tư và xây dựng trung tâm nghiên cứu tại tỉnh theo quy định pháp luật.

Rà soát, đơn giản hóa quy trình, tạo hành lang pháp lý thông thoáng để doanh nghiệp khoa học công nghệ tham gia cung cấp dịch vụ, giải pháp an ninh mạng cho các cơ quan Đảng và Nhà nước trên địa bàn.

Tham mưu Quy chế phối hợp giữa các lực lượng thực hiện nhiệm vụ bảo vệ an ninh mạng, phòng chống tội phạm công nghệ cao và bảo đảm an toàn thông tin mạng trên địa bàn tỉnh theo mô hình tập trung, thống nhất. Xây dựng Kế hoạch triển khai chương trình đào tạo và diễn tập thực chiến ứng phó sự cố an ninh mạng trên địa bàn tỉnh.

- Về hạ tầng: Xây dựng và phát triển hạ tầng an ninh mạng của tỉnh theo hướng hiện đại, đồng bộ đảm bảo an toàn, an ninh thông tin.

- 100% hệ thống thông tin của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội tỉnh được rà soát, khắc phục các lỗ hổng, điểm yếu an ninh mạng.

- 100% hệ thống thông tin quan trọng cấp độ 3 trở lên (trừ quân sự, quốc phòng, cơ yếu) trên địa bàn tỉnh hoàn thành việc kết nối, chia sẻ dữ liệu giám sát với Trung tâm giám sát an ninh mạng (SOC) tỉnh và Trung tâm an ninh mạng quốc gia.

- Triển khai áp dụng và tuân thủ nghiêm ngặt các tiêu chuẩn, quy chuẩn kỹ thuật quốc gia đối với các sản phẩm, dịch vụ an ninh mạng; 100% trang thiết bị được rà soát, kiểm tra an ninh, an toàn thông tin trước khi đưa vào sử dụng.

- Bảo đảm hạ tầng kỹ thuật để triển khai các sản phẩm mật mã của ngành Cơ yếu ổn định, thông suốt, phục vụ trao đổi dữ liệu bí mật nhà nước từ tỉnh đến 100% các xã, phường, đặc khu và từ tỉnh lên Trung ương.

- **Về nhân lực:** 100% cán bộ, công chức, viên chức được tuyên truyền, có đủ thông tin để nhận diện lừa đảo trực tuyến, bảo mật thông tin cá nhân và quy tắc ứng xử an toàn trên không gian mạng. Tổ chức các lớp bồi dưỡng nâng cao kiến thức về an toàn thông tin mạng. Thực hành điều tra, ứng phó sự cố lây nhiễm mã độc; diễn tập đối kháng tấn công phòng thủ.

Nâng cao hiệu quả Tổ công nghệ số cộng đồng tại các xã, phường, thị trấn để tổ chức các chiến dịch truyền thông "đi từng ngõ, gõ từng nhà" về an ninh mạng; phấn đấu mỗi hộ gia đình có ít nhất một người có kiến thức cơ bản về phòng chống tội phạm mạng.

Kiện toàn và nâng cao năng lực cho Đội ứng cứu sự cố an toàn thông tin mạng của tỉnh; phấn đấu mỗi sở, ban, ngành và UBND cấp xã có ít nhất 01 cán bộ chuyên trách có chứng chỉ chuyên môn về an ninh mạng theo tiêu chuẩn quốc gia. Liên kết với các cơ sở đào tạo uy tín và các doanh nghiệp an ninh mạng hàng đầu Việt Nam để tổ chức các chương trình đào tạo chuyên sâu về quản trị hệ thống, diễn tập thực chiến cho đội ngũ chuyên gia của tỉnh.

- **Về quản trị:** Gắn kết quả bảo đảm an ninh mạng vào kết quả hoàn thành nhiệm vụ hằng năm của người đứng đầu các cơ quan, đơn vị.

100% các hệ thống thông tin của tỉnh phải được phê duyệt hồ sơ đề xuất cấp độ và triển khai đầy đủ phương án bảo đảm an toàn hệ thống thông tin theo cấp độ đã được phê duyệt (từ cấp độ 1 đến cấp độ 5 tùy tính chất hệ thống).

Tổ chức các đợt kiểm tra liên ngành về việc tuân thủ các quy chuẩn, tiêu chuẩn kỹ thuật quốc gia về an ninh mạng tại các đơn vị trọng yếu; kịp thời phát hiện và xử lý nghiêm các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân và bí mật nhà nước trên không gian mạng.

Duy trì và cập nhật quy trình phối hợp ứng cứu sự cố an ninh mạng giữa các đơn vị (theo mô hình 4 lớp), đảm bảo mọi sự cố phải được ghi nhận, phân tích rủi ro và có biện pháp xử lý đảm bảo theo quy định.

- **Về công nghệ:** Tích hợp công nghệ trí tuệ nhân tạo (AI) và phân tích dữ liệu lớn (Big Data) vào Trung tâm giám sát điều hành an toàn thông tin (SOC) của tỉnh để tự động hóa việc nhận diện hành vi bất thường và phân loại các cuộc

tấn công mạng theo thời gian thực.

Triển khai, thay thế mô hình phòng thủ truyền thống bằng mô hình Zero Trust (luôn luôn xác minh) đối với các hệ thống truy cập vào cơ sở dữ liệu dùng chung của tỉnh. Chủ động phát hiện các mã độc đã nằm vùng trong hệ thống. Đảm bảo 100% các giao dịch hành chính công trực tuyến cấp độ cao được bảo vệ bằng chữ ký số và các giao thức bảo mật lớp truyền tải mới nhất.

Khuyến khích các doanh nghiệp công nghệ trong nước tham gia cung cấp các dịch vụ kiểm thử an ninh mạng, đánh giá an toàn thông tin theo hình thức thuê dịch vụ chuyên nghiệp. Tạo điều kiện để các cơ sở nghiên cứu thí điểm các giải pháp bảo mật mới cho hệ thống giám sát môi trường biển và du lịch thông minh của tỉnh.

b) Mục tiêu đến năm 2030

- **Về nâng cao chỉ số an toàn, an ninh mạng**: Khánh Hòa phấn đấu nằm trong nhóm tỉnh dẫn đầu cả nước về bảo đảm an toàn, an ninh không gian mạng, an ninh dữ liệu và bảo vệ dữ liệu. Góp phần nâng cao năng lực an toàn thông tin quốc gia thông qua việc cải thiện thực chất các chỉ số thành phần trong Bộ chỉ số chuyển đổi số (DTI) và Chỉ số đổi mới sáng tạo (PII) cấp tỉnh. Tập trung bảo vệ tuyệt đối an toàn không gian mạng cho các hệ thống thông tin dùng chung của tỉnh, các cơ sở dữ liệu chuyên ngành và hạ tầng số phục vụ phát triển kinh tế biển, du lịch thông minh và sản xuất công nghệ cao, những lĩnh vực trọng điểm được xác định tại Nghị quyết số 48-NQ/TU, ngày 20/02/2025 của Tỉnh ủy.

- **Về thể chế:** Chủ động rà soát, tham mưu, đề xuất xây dựng các cơ chế, chính sách đặc thù của tỉnh nhằm khuyến khích đổi mới sáng tạo, tạo điều kiện cho doanh nghiệp khoa học công nghệ tham gia thị trường, sản phẩm, giải pháp an ninh mạng chất lượng có cơ hội phát triển. Thực hiện nghiêm các quy định của pháp luật bảo đảm đủ sức răn đe và phản ứng nhanh với các hành vi vi phạm pháp luật trên không gian mạng.

- **Về hạ tầng:** Xây dựng và đưa vào vận hành hiệu quả kiến trúc bảo vệ an ninh mạng đa lớp hiện đại, đồng bộ, hiệu quả góp phần đảm bảo vững chắc chủ quyền quốc gia trên không gian mạng, bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; triển khai và thực hiện nghiêm quy hoạch hạ tầng công nghệ thông tin tổng thể từ Trung ương đến địa phương theo yêu cầu của Trung ương.

- **Về nhân lực:** Xây dựng và triển khai lộ trình đào tạo, bồi dưỡng chuyên sâu, phấn đấu để tỉnh Khánh Hòa đóng góp tỷ lệ tương xứng vào chỉ tiêu 10.000 chuyên gia an ninh mạng trình độ cao của cả nước; bảo đảm nguồn nhân lực tại chỗ đáp ứng yêu cầu bảo vệ các hệ thống thông tin trọng yếu của tỉnh.

- **Về quản trị:** Các sở, ban, ngành, địa phương và các tổ chức vận hành hạ tầng thông tin quan trọng trên địa bàn tỉnh triển khai, áp dụng hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia.

- **Về công nghệ:** Ưu tiên sử dụng các sản phẩm, giải pháp và dịch vụ an ninh mạng sản xuất trong nước (Make in Vietnam) trong các dự án đầu tư mới và nâng cấp hệ thống. Phấn đấu đến năm 2030, tỷ trọng sản phẩm, dịch vụ an ninh mạng nội địa chiếm trên 50% tổng danh mục trang thiết bị, phần mềm tại các cơ quan Đảng và Nhà nước trên địa bàn tỉnh; từng bước hình thành hệ sinh thái công nghệ an ninh mạng tự chủ tại địa phương.

c) Tầm nhìn chiến lược đến năm 2045: Xây dựng nền an ninh mạng của tỉnh Khánh Hòa phát triển bền vững, tự chủ, hiện đại. Hình thành đội ngũ chuyên gia, nhà khoa học đầu ngành về an ninh mạng tại địa phương. Thúc đẩy các doanh nghiệp công nghệ số của tỉnh phát triển lớn mạnh, trở thành trụ cột quan trọng trong hệ sinh thái công nghiệp an ninh mạng, góp phần bảo đảm vững chắc chủ quyền số quốc gia và phát triển kinh tế - xã hội của tỉnh.

3. Yêu cầu

- Kế hoạch phải được quán triệt đến từng chi bộ, cơ quan, đơn vị; đảm bảo sự phối hợp chặt chẽ, đồng bộ giữa lực lượng Công an, Quân đội và các cấp ủy, sở, ban, ngành, địa phương, tuyệt đối không để xảy ra tình trạng khoán trách nhiệm cho các đơn vị chuyên trách.

- Các nhiệm vụ đề ra phải gắn liền với danh mục sản phẩm cụ thể (đề án, quy chế, phần mềm, báo cáo kỹ thuật); lộ trình thực hiện được định lượng hóa và kiểm soát tiến độ, định kỳ báo cáo kết quả về Ban Chỉ đạo tỉnh.

- Ưu tiên sử dụng các giải pháp công nghệ trong nước kết hợp với việc tiếp thu có chọn lọc các tiêu chuẩn kỹ thuật quốc tế để giải quyết các bài toán đặc thù của tỉnh về an toàn thông tin trong các ngành trọng điểm trên địa bàn tỉnh.

- Kết quả thực hiện công tác bảo mật, an ninh mạng là tiêu chí cứng trong đánh giá xếp loại chất lượng hằng năm và xét thi đua, khen thưởng đối với tập thể, cá nhân, đặc biệt là người đứng đầu cơ quan, đơn vị. Trường hợp để xảy ra sự cố nghiêm trọng do thiếu trách nhiệm phải xem xét xử lý theo quy định về kỷ luật Đảng và pháp luật Nhà nước.

II. NHIỆM VỤ TRỌNG TÂM NĂM 2026

1. Tiếp tục củng cố, kiện toàn và nâng cao chất lượng hoạt động của Tiểu ban An ninh mạng tỉnh. Rà soát quy chế hoạt động, phân công nhiệm vụ cụ thể cho các thành viên gắn với trách nhiệm quản lý địa bàn, lĩnh vực; bảo đảm mô hình hoạt động thực chất, hiệu quả, đúng chức năng, nhiệm vụ, phù hợp với mô hình chính quyền địa phương 2 cấp; khắc phục triệt để tình trạng hoạt động hình

thức, kiêm nhiệm nhưng không nắm chuyên môn. Rà soát, ban hành Quy chế phối hợp giữa các lực lượng thực hiện nhiệm vụ bảo vệ an ninh mạng, phòng chống tội phạm công nghệ cao và bảo đảm an toàn thông tin 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 từ tỉnh đến cơ sở có trách nhiệm: *(i)* 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. *(ii)* Triển khai giám sát an ninh mạng tại cơ quan, đơn vị thuộc phạm vi quản lý. *(iii)* 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. *(iv)* Xác định trách nhiệm của người đứng đầu về an ninh mạng.

3. Xây dựng và hoàn thiện Trung tâm giám sát an ninh mạng tỉnh Khánh Hòa; thực hiện 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) về Trung tâm giám sát an ninh mạng tỉnh và Trung tâm An ninh mạng quốc gia (Bộ Công an); 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. Kết nối, tham gia vào 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, ngành, địa phương, doanh nghiệp trên địa bàn tỉnh.

5. Ban hành Quy chế bảo đảm an ninh mạng trên địa bàn tỉnh; ban hành các quy định, tài liệu hướng dẫn về bảo đảm an ninh mạng, an toàn thông tin cho các cơ sở dữ liệu, hệ thống dùng chung trong hệ thống chính trị tỉnh; định kỳ tổ chức kiểm tra, đánh giá việc thực hiện các quy định bảo đảm an ninh mạng, an toàn thông tin; đồng thời tăng cường công tác thanh tra đột xuất và kiên quyết xử lý nghiêm các trường hợp vi phạm pháp luật về bảo vệ bí mật nhà nước trên không gian mạng.

6. Ban hành cơ chế ưu đãi đặc biệt và chính sách ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng, bảo mật thông tin và an ninh dữ liệu "Made in Vietnam"*;* từng bước hình thành hệ sinh thái an ninh mạng vững mạnh, nâng cao năng lực cạnh tranh.

7. 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 tỉnh đến cơ sở 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.

8. Rà soát, kiện toàn và bố trí đủ cán bộ chuyên trách hoặc kiêm nhiệm về an toàn, an ninh mạng tại 100% cơ quan, đơn vị; đặc biệt là tại đơn vị chuyên trách về an ninh mạng; bảo đảm cán bộ được hưởng đầy đủ chế độ, phụ cấp theo quy định.

II. NHIỆM VỤ ĐẾN NĂM 2030

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

a) Triển khai đồng bộ các khóa bồi dưỡng kỹ năng an toàn thông tin cơ bản cho cán bộ và nhân dân qua nền tảng số của tỉnh. Thiết lập kênh cảnh báo lừa đảo trực tuyến 24/7 trên các nền tảng mạng xã hội phổ biến và hệ thống loa truyền thanh cơ sở tại địa phương. Tích hợp kỹ năng nhận diện nguy cơ trên không gian mạng vào chương trình ngoại khóa và các môn học liên quan cho học sinh, sinh viên các cấp trên địa bàn tỉnh.

b) Thực hiện định danh và công khai mức độ tín nhiệm mạng đối với các trang thông tin, tổ chức và cá nhân có sức ảnh hưởng trên không gian mạng tại địa phương nhằm bảo vệ người dùng. Áp dụng bộ chỉ số đánh giá an toàn thông tin làm tiêu chí bắt buộc trong xếp loại chất lượng và xét khen thưởng hằng năm cho các cơ quan, đơn vị.

2. Góp ý xây dựng và hoàn thiện thể chế, khung pháp lý

a) Chủ động rà soát, đóng góp ý kiến để hoàn thiện hệ thống pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật về an ninh mạng, bảo mật thông tin, an ninh dữ liệu do Trung ương ban hành.

b) Tổ chức phổ biến, hướng dẫn và giám sát việc tuân thủ nghiêm ngặt các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật đối với các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin tại địa phương; áp dụng trước hết đối với hạ tầng các hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin của cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội trên địa bàn tỉnh có ảnh hưởng trực tiếp đến an ninh trật tự và đời sống Nhân dân.

c) Xây dựng và áp dụng Khung quản trị rủi ro an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý của tỉnh, bảo đảm đồng bộ với Khung quản trị rủi ro an ninh mạng quốc gia; tổ chức thực hiện bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng.

d) Vận hành hiệu quả cơ chế phối hợp, chia sẻ thông tin cảnh báo sớm và điều phối ứng cứu sự cố mạng giữa các cơ quan trong hệ thống chính trị tỉnh; đồng thời duy trì kết nối kỹ thuật liên tục với các trung tâm an ninh mạng quốc gia để tiếp nhận và xử lý kịp thời các nguy cơ bên ngoài.

3. Phát triển hạ tầng an ninh mạng hiện đại, đồng bộ, góp phần đáp ứng yêu cầu bảo vệ chủ quyền quốc gia trên không gian mạng

a) Triển khai các giải pháp bảo đảm an ninh mạng theo mô hình "4 lớp" tại tất cả các cơ quan trong hệ thống chính trị tỉnh. Trọng tâm là kết nối đồng bộ hạ tầng mạng của khối Đảng, chính quyền, Mặt trận Tổ quốc và các đoàn thể về Trung tâm Giám sát điều hành an toàn thông tin (SOC) tập trung của tỉnh để quản lý thống nhất.

b) Tối ưu hóa và bảo mật mạng diện rộng (WAN) của tỉnh, đảm bảo các kết nối từ cấp tỉnh đến 100% các xã, phường, đặc khu được giám sát và bảo vệ bằng tường lửa thế hệ mới và các sản phẩm mật mã chuyên dụng. Triển khai giải pháp phòng chống mã độc tập trung (Endpoint) và quản lý thiết bị di động cho 100% máy tính, thiết bị di động tham gia vào quy trình xử lý hồ sơ công vụ, dịch vụ công trực tuyến của tỉnh. Thực hiện kiểm tra, đánh giá an ninh mạng định kỳ đối với các hệ thống thông tin quan trọng trên địa bàn tỉnh, trong đó chú trọng hệ thống thông tin phục vụ hành chính công, các hệ thống điều hành thông minh (IOC) và các cơ sở dữ liệu quan trọng trên địa bàn tỉnh.

Thực hiện mã hóa các cơ sở dữ liệu dùng và triển khai mô hình kiểm soát truy cập "Zero Trust" (luôn xác minh) đối với cán bộ khi khai thác dữ liệu ngành, lĩnh vực. Thiết lập kênh phản hồi nhanh để hỗ trợ cán bộ, công chức và người dân xử lý các sự cố mất an toàn thông tin; đồng thời triển khai cơ chế định danh, đánh giá tín nhiệm mạng cho các nền tảng tương tác của chính quyền tỉnh.

c) Tăng cường năng lực tự chủ, thúc đẩy ứng dụng mạnh mẽ các công nghệ lõi, công nghệ mới đã được nghiên cứu, sản xuất trong nước vào thực tiễn quản lý và vận hành hệ thống của tỉnh; khuyến khích xã hội hóa nghiên cứu, phát triển và ứng dụng sản phẩm mật mã dân sự phục vụ bảo mật thông tin.

4. Tạo điều kiện phát triển công nghiệp an ninh mạng tự chủ và thị trường an ninh mạng cạnh tranh, minh bạch

a) Cụ thể hóa và triển khai hiệu quả các cơ chế đầu tư cho phát triển hệ sinh thái an ninh mạng, khuyến khích các doanh nghiệp công nghệ trong nước tham gia chuỗi cung ứng sản phẩm, dịch vụ an toàn thông tin mạng "Made in Vietnam". Ưu tiên bố trí nguồn lực, kinh phí để mua sắm, trang bị và triển khai các sản phẩm, giải pháp an ninh mạng cốt lõi, nền tảng do doanh nghiệp Việt Nam làm chủ công nghệ (đạt chuẩn quy định).

b) Chủ động thiết lập các không gian khởi nghiệp và vườn ươm công nghệ số tại Nha Trang và các khu kinh tế trọng điểm để hỗ trợ doanh nghiệp công nghệ địa phương nghiên cứu, ứng dụng và thương mại hóa các giải pháp bảo mật. Tập

trung tạo lập môi trường kinh doanh minh bạch, tạo điều kiện cho các doanh nghiệp vừa và nhỏ của tỉnh tiếp cận thị trường cung ứng dịch vụ an toàn thông tin.

c) Thực hiện chính sách ưu tiên đầu tư, mua sắm các sản phẩm và dịch vụ an ninh mạng sản xuất trong nước đã được kiểm định đối với các dự án hạ tầng số và hệ thống thông tin trọng yếu của tỉnh. Việc ưu tiên này nhằm tạo thị trường tại chỗ, thúc đẩy các doanh nghiệp Việt Nam phát triển và trực tiếp góp phần nâng cao năng lực tự chủ chiến lược về công nghệ của tỉnh và quốc gia.

d) Tổ chức phổ biến, hướng dẫn và giám sát việc áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật về mật mã dân sự đối với các hệ thống thông tin của cơ quan Đảng, Nhà nước và các tổ chức kinh tế - xã hội trên địa bàn tỉnh. Đảm bảo việc sử dụng các giải pháp mã hóa đạt chuẩn quốc gia để bảo vệ dữ liệu công vụ, giao dịch điện tử và thông tin cá nhân của người dân trước các nguy cơ tấn công mạng.

5. Bảo đảm nguồn lực tài chính, ngân sách

Quy định việc thẩm định an ninh mạng, bảo mật và an toàn dữ liệu là nội dung bắt buộc, không thể tách rời trong hồ sơ đề xuất chủ trương đầu tư của mọi dự án công nghệ thông tin trên địa bàn tỉnh. Ưu tiên bố trí ngân sách cho các hạng mục an toàn thông tin với tỷ lệ kinh phí đạt tối thiểu 15% tổng mức đầu tư của các đề án, kế hoạch ứng dụng công nghệ thông tin; đảm bảo nguồn kinh phí này được sử dụng tập trung, có trọng điểm và tránh dàn trải.

Thường xuyên rà soát, tổng hợp các vướng mắc thực tiễn về định mức, đơn giá và thủ tục đấu thầu đặc thù trong lĩnh vực an ninh mạng để chủ động tham mưu, kiến nghị cấp có thẩm quyền ban hành các cơ chế tài chính linh hoạt, giúp đẩy nhanh tiến độ triển khai các nhiệm vụ bảo mật cấp bách của tỉnh.

6. Bảo đảm nguồn nhân lực

a) Rà soát, tham mưu ban hành các cơ chế, chính sách đặc thù của tỉnh để thu hút, đãi ngộ các chuyên gia, nhân lực chất lượng cao tham gia tư vấn, hỗ trợ và phục vụ công tác bảo đảm an ninh mạng trên địa bàn tỉnh.

b) Tổ chức các chương trình huấn luyện thực tế về kỹ năng giám sát, điều tra số và ứng cứu sự cố an ninh mạng cho đội ngũ cán bộ chuyên trách của tỉnh. Định kỳ tổ chức các đợt diễn tập đối kháng và xử lý tình huống lây nhiễm mã độc trên các hệ thống thông tin dùng chung để nâng cao khả năng phản ứng nhanh của Đội ứng cứu sự cố tỉnh. Bồi dưỡng năng lực vận hành, quản trị và khai thác hiệu quả các thiết bị an ninh mạng hiện đại, các công nghệ lõi và nền tảng giám sát tập trung (SOC) đã được đầu tư tại địa phương. Tập trung đào tạo các kỹ thuật bảo mật, mã hóa và quản trị an toàn dữ liệu cho cán bộ trực tiếp vận hành các cơ sở dữ liệu của tỉnh.

c) Tăng cường liên kết giữa *"Nhà nước - Nhà trường - Doanh nghiệp"* trong đào tạo, huấn luyện thực chiến. Xây dựng và mở rộng mạng lưới chuyên gia an ninh mạng của tỉnh, huy động sự tham gia của các chuyên gia giỏi để hỗ trợ ứng cứu sự cố và tham gia bảo vệ các hệ thống trọng yếu.

d) Tăng cường nhân lực bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho các cơ quan, đơn vị, địa phương theo quy định.

7. Triển khai hợp tác về an ninh mạng

Chủ động cập nhật và triển khai áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật quốc gia phù hợp với chuẩn mực quốc tế trong vận hành các hệ thống thông tin của tỉnh; đảm bảo tính tương thích và an toàn khi kết nối các hạ tầng số địa phương với môi trường mạng toàn cầu.

Triển khai có hiệu quả các nội dung phối hợp theo định hướng của Công ước Hà Nội về chống tội phạm mạng năm 2025; tập trung vào việc chuẩn bị các điều kiện kỹ thuật, pháp lý tại địa phương để sẵn sàng phối hợp điều tra, xử lý tội phạm mạng theo điều phối của cơ quan Trung ương.

Tăng cường trao đổi thông tin về các thủ đoạn tội phạm mạng mới, qua các kênh chính thống của ngành Công an; lựa chọn và cử cán bộ chuyên trách có trình độ tham gia các chương trình đào tạo, huấn luyện chuyên sâu và diễn tập quốc tế do các bộ, ngành Trung ương tổ chức nhằm làm chủ các công nghệ bảo mật tiên tiến hiện nay.

III. TỔ CHỨC THỰC HIỆN

1. Phân công trách nhiệm: *(Chi tiết tại phụ lục đính kèm)*

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 trước ngày 25 hằng tháng trên Hệ thống thông tin giám sát, đánh giá việc thực hiện Nghị quyết số 57-NQ/TW (https://theodoinq.dcs.vn).

4. Tổng kết, đánh giá và khen thưởng kỷ luật

- Gắn kết quả thực hiện Kế hoạch với đánh giá, xếp loại mức độ hoàn thành nhiệm vụ của tập thể và cá nhân, đặc biệt là người đứng đầu.

- Kịp thời biểu dương, khen thưởng các tập thể, cá nhân có thành tích xuất sắc, các mô hình hay, cách làm sáng tạo; đồng thời xem xét, xử lý nghiêm các trường hợp không hoàn thành nhiệm vụ, thiếu trách nhiệm, gây ảnh hưởng đến các mục tiêu chung của Kế hoạch.

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

Nơi nhận:
- Ban Thường vụ Tỉnh ủy,
- Thành viên Ban Chỉ đạo tỉnh,
- Các cơ quan tham mưu, giúp việc Tỉnh ủy,
- Các Đảng ủy trực thuộc Tỉnh ủy,
- MTTQ và các tổ chức chính trị - xã hội tỉnh,
- Thường trực Bộ phận giúp việc Ban Chỉ đạo,
- Tòa án nhân dân tỉnh, Viện Kiểm sát nhân dân tỉnh (để phối hợp),
- Lưu Văn phòng Tỉnh ủy.

BÍ THƯ
kiêm
TRƯỞNG BAN CHỈ ĐẠO

TỈNH UỶ KHÁNH HÒA
16-03-2026 09:47:37 +07:00

ĐẢNG CỘNG SẢN VIỆT NAM
TỈNH ỦY KHÁNH HÒA

Nghiêm Xuân Thành

PHỤ LỤC
Phân công nhiệm vụ các cơ quan đơn vị triển khai thực hiện Kế hoạch
(Ban hành kèm theo Kế hoạch số 07-KH/BCĐ, ngày 16/3/2026 của Ban Chỉ đạo 57 tỉnh)

STT	Đơn vị thực hiện	Nhiệm vụ	Thời hạn hoàn thành	Ghi chú/ cơ quan phối hợp
01	Ban Chỉ đạo tỉnh	Chỉ đạo toàn diện, cho ý kiến về chủ trương/cơ chế lớn, tháo gỡ khó khăn liên ngành	**Thường xuyên**	Trực tiếp lãnh đạo toàn tỉnh
02	Thường trực Ban Chỉ đạo	Chỉ đạo, điều hành trực tiếp, giao ban định kỳ, đôn đốc, kiểm tra, giám sát tiến độ triển khai Kế hoạch	**Thường xuyên**	Phối hợp Cơ quan Thường trực Tiểu ban An ninh mạng
03	Đảng ủy các cơ quan Đảng, UBND, MTTQ, các tổ chức chính trị - xã hội tỉnh	Cụ thể hoá các cơ chế, thể chế, ban hành văn bản hướng dẫn; tổ chức triển khai 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.	**Thường xuyên**	Các cơ quan, đơn vị liên quan
04		Thực hiện kết nối, liên thông các hệ thống thông tin phục vụ chỉ đạo, điều hành (quản lý văn bản, hồ sơ công việc, hệ thống báo cáo, họp trực tuyến) của các khối cơ quan Đảng, HĐND, UBND, MTTQ, các tổ chức chính trị - xã hội, Toà án nhân dân và Viện kiểm sát nhân dân tỉnh bảo đảm an toàn và bảo mật thông tin.	**Tháng 4/2026**	Các cơ quan, đơn vị liên quan
05		Ban hành quy định và hướng dẫn các đơn vị trực thuộc ưu tiên sử dụng sản phẩm, dịch vụ an ninh mạng, an toàn thông tin "Make in Vietnam" đáp ứng yêu cầu bảo đảm an ninh mạng, bảo mật dữ liệu và an toàn thông tin.	**Triển khai thực hiện ngay sau khi Trung ương có hướng dẫn, quy định cụ thể.**	Các cơ quan, đơn vị liên quan
06	**Đảng ủy UBND tỉnh (chỉ đạo UBND tỉnh)**	Chỉ đạo UBND tỉnh, giao Văn phòng UBND	**Thường xuyên**	

		tỉnh chủ trì, phối hợp chặt chẽ với Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh và Sở Khoa học và Công nghệ trong việc tham mưu thực hiện các hoạt động đối ngoại về an ninh mạng và các công nghệ mới.		
07	**Đảng uỷ Công an tỉnh** ***(chỉ đạo Công an tỉnh)***	Chủ trì công tác ham mưu quản lý nhà nước về an ninh mạng (trừ lĩnh vực quân sự, quốc phòng, cơ yếu); đề xuất 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 Giữ vai trò cơ quan thường trực về bảo đảm an ninh mạng, bảo mật thông tin và dữ liệu trong cả hệ thống chính trị.	**Nhiệm vụ thường xuyên**	Các cơ quan, đơn vị liên quan
08		Hoàn thành vận hành Trung tâm Giám sát an ninh mạng tỉnh (SOC); thiết lập kênh kết nối, chia sẻ dữ liệu giám sát, cảnh báo với Trung tâm An ninh mạng quốc gia (Bộ Công an) đối với hệ thống thông tin quan trọng cấp độ 3 trở lên (trừ quân sự, quốc phòng, cơ yếu); đồng thời thiết lập kênh trao đổi thông tin phục vụ giám sát, điều phối ứng cứu và khắc phục sự cố an ninh mạng trong phạm vi quản lý.	**Hoàn thành SOC giai đoạn 1 trước 30/06/2026 và hoàn thiện SOC trong năm 2027.**	Sở Khoa học và Công nghệ, các cơ quan, đơn vị liên quan
09		Tăng cường thanh tra, kiểm tra đột xuất việc chấp hành pháp luật bảo vệ bí mật nhà nước trên không gian mạng; kiên quyết chấn chỉnh, xử lý nghiêm vi phạm do lỗi chủ quan như soạn thảo văn bản mật trên máy kết nối	**Thực hiện đợt cao điểm hoàn thành trong tháng 6/2026; sau đó duy trì thường xuyên.**	

		Internet, dùng thiết bị lưu trữ ngoài không an toàn, cài phần mềm không rõ nguồn gốc... (Căn cứ Công văn 261/X05-P5 ngày 27/01/2026 của Thanh tra Bộ Công an và Công văn 2336/UBND-NC ngày 06/02/2026).		
10		Tham gia 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, ngành, địa phương, doanh nghiệp.	**Triển khai theo lộ trình và hướng dẫn kỹ thuật của Bộ Công an (dự kiến hoàn thành trong tháng 03/2027).**	Các cơ quan, ban, ngành, địa phương, doanh nghiệp
11		Chủ trì, phối hợp với Sở Khoa học và Công nghệ và các cơ quan, đơn vị, địa phương: (i) Xây dựng, ban hành văn bản hướng dẫn các cơ quan, đơn vị, địa phương triển khai áp dụng TCVN mới về An ninh mạng ngay sau khi được Trung ương công bố; định kỳ hằng năm chủ trì tổ chức kiểm tra, đánh giá việc tuân thủ, áp dụng TCVN tại các đơn vị.	**Nhiệm vụ thường xuyên**	Sở Khoa học và Công nghệ và các cơ quan, đơn vị liên quan
12		Tổ chức chiến dịch truyền thông mạnh mẽ trên truyền hình, báo chí, thông tin cơ sở, mạng xã hội, kết hợp cảnh báo trực tiếp qua nhà mạng, ngân hàng và nền tảng số; phổ cập kỹ năng an toàn số cho người dân qua giáo dục, tập huấn cộng đồng và tài liệu trực tuyến. Thiết lập, vận hành kênh tiếp nhận - xử lý phản ánh an ninh mạng 24/7 liên thông giữa cơ quan chức năng, doanh nghiệp và người dân nhằm kịp thời phát hiện, ngăn chặn lừa đảo trực tuyến.	**Tháng 4/2026**	Sở Khoa học và Công nghệ và các cơ quan, đơn vị liên quan

13		Chủ trì, phối hợp với Sở Khoa học và Công nghệ và các cơ quan liên quan: (i) Tham mưu xây dựng, ban hành Khung quản trị rủi ro an ninh mạng tỉnh trên cơ sở Khung quản trị rủi ro an ninh mạng quốc gia. (ii) Xây dựng bộ chỉ số bảo đảm an ninh mạng làm cơ sở đánh giá năng lực bảo đảm an ninh mạng của các sở, ban, ngành, địa phương, tổ chức, doanh nghiệp hằng năm; tổ chức xếp hạng về công tác an ninh mạng đối với các cơ quan, đơn vị để phục vụ đánh giá, xếp hạng chung về phát triển khoa học, công nghệ, chuyển đổi số của tỉnh.	**Hoàn thành trong năm 2026, áp dụng từ năm 2027**	Sở Khoa học và Công nghệ và các cơ quan, đơn vị liên quan
14		Chủ trì, phối hợp với Sở Khoa học và Công nghệ hướng dẫn các đơn vị, địa phương triển khai, ứng dụng nền tảng điều hành hạ tầng điện toán đám mây do Việt Nam làm chủ đáp ứng các yêu cầu an ninh mạng	**Hoàn thành trong năm 2026.**	Sở Khoa học và Công nghệ và các cơ quan, đơn vị liên quan
15		Chủ trì, phối hợp với Sở Tài chính, Sở Khoa học và Công nghệ và các cơ quan liên quan rà soát, tham mưu UBND tỉnh ban hành quy định hoặc văn bản hướng dẫn xác 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.	**Tháng 4/2026**	Sở Tài chính, Sở Khoa học và Công nghệ và các cơ quan liên quan
16		Xây dựng cơ chế hậu kiểm và đánh giá hiệu quả việc thực hiện chi tiêu tối thiểu 15% ngân	**Tháng 12/2026**	Sở Tài chính, Sở Khoa học và Công nghệ và các

		sách cho an ninh mạng; trong đó ưu tiên sử dụng cho các sản phẩm *"Make in Vietnam"* đã qua kiểm định, đánh giá chất lượng.		cơ quan liên quan
17		Chủ trì, phối hợp Sở Nội vụ, Sở Khoa học và Công nghệ, Sở Giáo dục và đào tạo và các đơn vị liên quan triển khai các khóa 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. 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. 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**	
18		Chủ trì, phối hợp với Viện Kiểm sát nhân dân tỉnh, Toà án nhân dân tỉnh rà soát, tham mưu sửa đổi, bổ sung các quy định của pháp luật yêu cầu các doanh nghiệp cung cấp dịch vụ tài chính, ngân hàng, viễn thông, Internet thực hiện kết nối kỹ thuật, cung cấp thông tin, dữ liệu, chứng cứ điện tử đầy đủ, kịp thời qua phương thức điện tử cho cơ quan chức năng, đơn giản hoá thủ tục hành chính nhằm bảo đảm thời gian phục vụ phòng ngừa, đấu tranh, ngăn chặn và xử lý các hành vi vi phạm pháp luật trên không gian mạng.	**Hoàn thành trong tháng 12/2026.**	Viện Kiểm sát tỉnh và Toà án nhân dân tỉnh

19		Xây dựng Phương án kiện toàn nhân sự đơn vị chuyên trách về an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao bảo đảm hoạt động hiệu lực, hiệu quả .	**Theo quy định, chỉ đạo của Bộ Công an và tình hình thực tiễn tại địa phương.**	Các cơ quan, đơn vị liên quan
20		- Tiếp tục đổi mới hình thức, biện pháp phổ biến, tuyên truyền các quy định của pháp luật về bảo vệ Bí mật nhà nước và An ninh mạng; tổ chức các lớp tập huấn chuyên sâu về công tác bảo vệ Bí mật nhà nước, nâng cao kiến thức về An ninh mạng và an toàn thông tin mạng cho cán bộ, công chức, viên chức được giao kiêm nhiệm thực hiện công tác bảo vệ Bí mật nhà nước và An ninh mạng tại các cơ quan, đơn vị trực thuộc. Tham mưu đầu tư nâng cấp cơ sở hạ tầng, trang thiết bị, công cụ, phương tiện kỹ thuật và các sản phẩm mật mã cơ yếu chuyên dụng phục vụ công tác bảo vệ bí mật nhà nước	**Hoàn thành trước tháng 06/2026**	Các cơ quan, đơn vị liên quan
21		Chủ trì, phối hợp với các đơn vị liên quan tổ chức quán triệt và triển khai thực hiện có hiệu quả, thực chất các nội dung của Công ước Hà Nội về chống tội phạm mạng năm 2025 theo hướng dẫn của Bộ Công an.	**Theo quy định, hướng dẫn của Bộ Công an**	Các cơ quan, đơn vị liên quan
22	**Đảng ủy Quân sự tỉnh (chỉ đạo Bộ Chỉ huy Quân sự tỉnh)**	Chịu trách nhiệm toàn diện trước Tỉnh ủy về công tác bảo đảm an ninh mạng, mật mã, bảo	**Nhiệm vụ thường xuyên.**	

		mật thông tin trong lĩnh vực quân sự, quốc phòng, cơ yếu thuộc phạm vi quản lý của Bộ Chỉ huy Quân sự tỉnh. Chỉ đạo công tác đảm bảo an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo phạm vi quản lý, chức năng, nhiệm vụ được giao.		
23		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 theo chức năng, nhiệm vụ được giao và trong lĩnh vực thuộc phạm vi quản lý (bao gồm cả hệ thống 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.**	Các cơ quan, đơn vị, doanh nghiệp liên quan
24		Căn cứ các tiêu chuẩn, quy chuẩn của Bộ Quốc phòng, chủ trì xây dựng và ban hành các quy định, yêu cầu kỹ thuật cụ thể đối với sản phẩm, dịch vụ an ninh mạng đưa vào sử dụng trong các cơ quan, đơn vị thuộc phạm vi quản lý của Bộ Chỉ huy Quân sự tỉnh.	**Triển khai thực hiện ngay sau khi Bộ Quốc phòng có hướng dẫn, quy định cụ thể.**	Các cơ quan, đơn vị liên quan
25		Chủ trì, phối hợp với Văn phòng Tỉnh ủy, Công an tỉnh, Sở Khoa học và Công nghệ và các đơn vị liên quan rà soát, khảo sát hiện trạng để phục vụ xây dựng và triển khai áp dụng Khung kiến trúc hạ tầng mật mã quốc gia tại tỉnh Khánh Hòa ngay sau khi được ban hành.	**Theo quy định, hướng dẫn của Ban Cơ yếu Chính phủ .**	Văn phòng Tỉnh uỷ, Công an tỉnh, Sở Khoa học và Công nghệ và các đơn vị liên quan

26		- Chủ trì, phối hợp với Văn phòng Tỉnh ủy bảo đảm hạ tầng mật mã hoạt động ổn định, an toàn; phục vụ hiệu quả việc bảo mật, trao đổi dữ liệu bí mật nhà nước thông suốt trong hệ thống chính trị của tỉnh từ cấp tỉnh đến 100% cấp xã.	**Nhiệm vụ thường xuyên.**	Văn phòng Tỉnh ủy
27		- Phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ tổ chức quán triệt, hướng dẫn và kiểm tra việc tuân thủ các tiêu chuẩn, quy chuẩn kỹ thuật về mật mã dân sự đối với các tổ chức, cá nhân sử dụng sản phẩm mật mã dân sự để bảo vệ an ninh mạng trên địa bàn tỉnh.	**Nhiệm vụ thường xuyên.**	Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan liên quan
28		- Chủ trì, phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan liên quan rà soát, đề xuất nhu cầu và lộ trình đăng ký tham gia thí điểm, ứng dụng các giải pháp bảo mật bằng công nghệ mã hoá kháng lượng tử *(theo hướng dẫn, chuyển giao của Bộ Quốc phòng và Ban Cơ yếu Chính phủ)*; tham mưu UBND tỉnh các giải pháp thúc đẩy xã hội hoá, khuyến khích các doanh nghiệp, tổ chức trên địa bàn tham gia nghiên cứu, phát triển và ưu tiên ứng dụng các sản phẩm mật mã dân sự để bảo vệ an ninh mạng.	**Theo hướng dẫn, quy định của Bộ Quốc phòng.**	Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan liên quan
29	**Đảng uỷ Sở Khoa học và Công nghệ (chỉ đạo Sở**	Chủ trì, phối hợp với Công an tỉnh và các đơn vị liên quan rà soát hiện trạng, tham mưu	**Triển khai thực hiện ngay sau khi Trung**	Công an tỉnh và các đơn vị liên quan

	Khoa học và Công nghệ)	UBND tỉnh phương án điều chỉnh quy hoạch hạ tầng thông tin của tỉnh; xây dựng lộ trình tập trung các máy chủ, hệ thống thông tin phân tán về Trung tâm dữ liệu của tỉnh (đảm bảo đạt chuẩn, đủ điều kiện an toàn) để thống nhất quản lý và triển khai các biện pháp bảo vệ an ninh mạng.	**ương có hướng dẫn, quy định cụ thể.**	
30		Chủ trì, phối hợp với Công an tỉnh và các cơ quan liên quan tổ chức phổ biến, hướng dẫn các sở, ban, ngành, địa phương áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an ninh mạng đối với sản phẩm, dịch vụ công nghệ *(Cloud, Chính phủ số, IoT/OT, AI, Blockchain, viễn thông)*; phối hợp Công an tỉnh tham mưu áp dụng TCVN 14423: 2025 *(sửa đổi)* ngay sau khi được ban hành để phù hợp với các cấp độ hệ thống thông tin theo Luật An ninh mạng trên địa bàn tỉnh.	**Triển khai thực hiện ngay sau khi Trung ương có hướng dẫn, quy định cụ thể.**	Công an tỉnh và các cơ quan liên quan
31		Phối hợp với Công an tỉnh hướng dẫn các cơ quan, đơn vị triển khai, ứng dụng nền tảng điều hành hạ tầng điện toán đám mây do Việt Nam làm chủ đáp ứng các yêu cầu an ninh mạng.	**Nhiệm vụ thường xuyên.**	Công an tỉnh
32		Chủ trì, phối hợp với các đơn vị liên quan tham mưu UBND tỉnh ban hành các cơ chế, chính sách đặc thù nhằm hỗ trợ, thúc đẩy các doanh nghiệp công nghệ số trên địa bàn tỉnh	**Triển khai thực hiện ngay sau khi Trung ương có hướng dẫn, quy định cụ thể.**	Các cơ quan, đơn vị liên quan

		tham gia nghiên cứu, làm chủ công nghệ và phát triển các sản phẩm *"Make in Vietnam"* phục vụ chuyển đổi số và an ninh mạng tại địa phương.		
33		Chủ trì, phối hợp với Công an tỉnh xây dựng, mở rộng và duy trì mạng lưới liên kết với các chuyên gia an ninh mạng (trong và ngoài tỉnh) để sẵn sàng huy động tham gia tư vấn, hỗ trợ ứng cứu, khắc phục sự cố an ninh mạng trên địa bàn tỉnh khi cần thiết.	**Nhiệm vụ thường xuyên.**	
34	**Đảng uỷ Sở Giáo dục và Đào tạo** *(chỉ đạo Sở Giáo dục và Đào tạo)*	Chủ trì rà soát, tham mưu triển khai chương trình đào tạo chuyên sâu về an ninh mạng và công nghệ lõi phù hợp với nhu cầu thực tiễn của tỉnh; phối hợp với Công an tỉnh và các đơn vị có liên quan 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 cơ quan, đơn vị, địa phương.	**Nhiệm vụ thường xuyên.**	
35		Chủ trì, phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ và các đơn vị có liên quan tổ chức triển khai, hướng dẫn khai thác các chương trình đào tạo, tập huấn trên nền tảng "Bình dân học vụ số" (do Bộ Giáo dục và Đào tạo ban hành); tổ chức các lớp bồi dưỡng kiến thức, kỹ năng sư phạm về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu	**Nhiệm vụ thường xuyên.**	

		cho đội ngũ cán bộ quản lý, giáo viên trong toàn ngành giáo dục của tỉnh.		
36		Chủ trì, phối hợp với Sở Khoa học và Công nghệ, Công an tỉnh xây dựng và ban hành hướng dẫn triển khai thực hiện "Khung Năng lực số và An toàn mạng Toàn diện" trong các nhà trường trên địa bàn tỉnh (ngay sau khi Bộ Giáo dục và Đào tạo ban hành); chủ động chỉ đạo lồng ghép, 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 hoạt động giáo dục, sinh hoạt ngoại khóa để hình thành văn hoá số an toàn từ sớm cho học sinh.	**Theo quy định, hướng dẫn của Bộ Giáo dục và Đào tạo.**	
37	**Đảng uỷ Sở Tài chính** *(chỉ đạo Sở Tài chính)*	Chủ trì, phối hợp với các cơ quan, đơn vị liên quan tham mưu UBND tỉnh cân đối, bố trí ngân sách tỉnh để bảo đảm nguồn lực tài chính cho các hoạt động bảo đảm an ninh mạng, đầu tư hạ tầng bảo mật thông tin và an ninh dữ liệu của các cơ quan, ban, ngành, địa phương.	**Nhiệm vụ thường xuyên**	
38		Chủ trì, phối hợp với các đơn vị liên quan rà soát, tham mưu UBND tỉnh ban hành văn bản hướng dẫn cụ thể về tài chính, công sản, ngân sách và đấu thầu để tạo thuận lợi trong quá trình triển khai thực tiễn, đáp ứng yêu cầu	**Triển khai thực hiện ngay sau khi Bộ Tài chính có hướng dẫn, quy định cụ thể (dự kiến thực hiện trong Quý**	

		nhiệm vụ và đặc thù vòng đời của sản phẩm giải pháp an ninh mạng thường ngắn hơn quy định về khấu hao công sản.	**II/2026).**	
39	**Ban Tuyên giáo và Dân vận Tỉnh ủy**	Chủ trì, phối hợp với các cơ quan liên quan trong việc 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.**	
40	**Các sở, ban, ngành, địa phương, doanh nghiệp nhà nước**	Khẩn trương kiện toàn, duy trì bộ phận hoặc cán bộ đầu mối chuyên trách an ninh mạng dưới sự chỉ đạo trực tiếp của Người đứng đầu cơ quan, đơn vị (trong đó Bí thư cấp ủy, Thủ trưởng cơ quan, đơn vị chịu trách nhiệm trực tiếp).	**Hoàn thành trong Quý I/2026.**	
41		Chủ trì, phối hợp với các đơn vị liên quan rà soát, đánh giá và củng cố lại Hệ thống giám sát an ninh mạng tại đơn vị mình; Công an tỉnh chủ trì, phối hợp với Sở Khoa học và Công nghệ thực hiện công tác giám sát, điều phối ứng phó, xử lý sự cố an ninh mạng tại địa phương.		
42		Sở Khoa học và Công nghệ cùng các đơn vị quản lý hệ thống dữ liệu dùng riêng chịu trách nhiệm giám sát an ninh mạng 24/7 đối với các hệ thống thông tin trọng yếu thuộc phạm vi	**Hoàn thành trong tháng 5/2026.**	

		quản lý. Chủ trì, phối hợp chặt chẽ với Công an tỉnh xây dựng phương án ứng cứu sự cố và thiết lập kênh chia sẻ dữ liệu giám sát tập trung, liên thông với hệ thống quốc gia. Thủ trưởng các cơ quan trực tiếp chỉ đạo bộ phận chuyên môn tham gia ứng phó, khắc phục sự cố kịp thời (trừ lĩnh vực quân sự, quốc phòng và cơ yếu).		
43		Chủ trì, phối hợp với các đơn vị liên quan tổ chức rà soát, đánh giá tổng thể về an ninh mạng, bảo mật thông tin và an ninh dữ liệu đối với các cơ sở dữ liệu quốc gia, chuyên ngành, hệ thống thông tin và nguồn nhân lực.	**Hoàn thành trong tháng 6/2026.**	
44		Chỉ đạo các cơ quan, đơn vị huy động mọi nguồn lực để khắc phục ngay những lỗ hổng bảo mật trong các hệ thống thông tin thuộc phạm vi quản lý. Chủ động triển khai tổng thể các giải pháp kỹ thuật để giám sát, bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu cho toàn bộ các hệ thống thông tin trong phạm vi quản lý của cơ quan, đơn vị mình.	**Hoàn thành trong tháng 4/2026.**	
45		Thực hiện nghiêm công tác bảo vệ bí mật nhà nước và an ninh mạng, nâng cao trách nhiệm người đứng đầu các cơ quan, tổ chức và đơn vị, gắn trách nhiệm bảo vệ bí mật nhà nước và an ninh mạng đối với từng cá nhân, tập thể trong soạn thảo, lưu giữ, quản lý, vận chuyển,	**Nhiệm vụ thường xuyên.**	

		bàn giao, cung cấp bí mật nhà nước và quản lý, sử dụng hệ thống thông tin an ninh mạng.		
46		Phối hợp với các đơn vị liên 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 các hạ tầng, hệ thống 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 phê duyệt đối với hệ thống quan trọng (cấp độ 3 trở lên) trong tháng 4/2026; các hệ thống còn lại hoàn thành trong tháng 6/2026.**	
47		Phối hợp với Công an tỉnh 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 theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng Công an tỉnh theo quy định (trừ các hệ thống thông tin trong lĩnh vực quân sự, quốc phòng và cơ yếu)	**Hoàn thành trong tháng 4/2026.**	
48		Thực hiện nghiêm chế độ báo cáo sự cố trong vòng 24 giờ và tuân thủ theo sự điều phối ứng phó của lực lượng chuyên trách bảo vệ an ninh mạng Công an tỉnh theo quy định	**Nhiệm vụ thường xuyên**	

49		Phối hợp Công an tỉnh rà soát, tham mưu UBND tỉnh sửa đổi, bổ sung các văn bản quy phạm pháp luật, quy định của tỉnh và hoàn thiện quy chế nội bộ về bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu và danh mục bảo vệ bí mật nhà nước để phù hợp với quy định mới tại Luật An ninh mạng, Luật Bảo vệ bí mật nhà nước.	**Nhiệm vụ thường xuyên.**	Công an tỉnh và các cơ quan, đơn vị liên quan
50		Triển khai toàn diện mô hình bảo đảm an toàn thông tin "4 lớp" cho các hệ thống thông tin thuộc phạm vi quản lý, 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 khách quan và minh bạch. (4) Kết nối, chia sẻ thông tin về Công an tỉnh, bảo đảm sự phối hợp liên thông với hệ thống giám sát an ninh mạng quốc gia (trừ các hệ thống thông tin quân sự, quốc phòng, cơ yếu).	**Hoàn thành trong tháng 4/2026**	Các cơ quan, đơn vị liên quan
51		Giao Công an tỉnh và Bộ Chỉ huy Quân sự tỉnh theo phạm vi quản lý, chức năng, nhiệm vụ được giao, chủ trì, phối hợp với Văn phòng Tỉnh ủy chuẩn bị tài liệu, báo cáo phục vụ các cuộc họp, buổi làm việc của Thường trực Ban Chỉ đạo tỉnh với các cơ quan liên quan về các	**Theo yêu cầu Thường trực Ban Chỉ đạo**	Các cơ quan, đơn vị liên quan

		nội dung, nhiệm vụ theo Kế hoạch này.		
52		Phải bảo đảm tích hợp đầy đủ yêu cầu về an toàn, an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong toàn bộ quá trình thiết kế, thẩm định và triển khai khi xây dựng, cập nhật hoặc hoàn thiện Khung kiến trúc số tỉnh Khánh Hòa.	**Nhiệm vụ thường xuyên**	Các cơ quan, đơn vị liên quan
53	**Người đứng đầu cấp ủy, chính quyền, cơ quan, đơn vị trên địa bàn tỉnh**	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, lọt 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 đầu, để phục vụ công tác xếp loại hàng năm. Triển khai chương trình đánh giá tín nhiệm mạng đối với các tổ chức, cá nhân có ảnh hưởng trên không gian mạng nhằm củng cố lòng tin của người dân trong quá trình hoạt động, tương tác và làm việc trên không gian mạng.	**Nhiệm vụ thường xuyên.**	Các cơ quan, đơn vị liên quan
54	**Các doanh nghiệp**	Tham gia chủ trì, đồng hành trong hoạt động chuyển đổi số tại các cơ quan, đơn vị, địa phương thuộc tỉnh có trách nhiệm phối hợp	**Nhiệm vụ thường xuyên**	Các cơ quan, đơn vị liên quan

		chặt chẽ với cơ quan, đơn vị chủ quản trong việc thực hiện đầy đủ các quy định của pháp luật về bảo đảm an ninh mạng, an toàn thông tin và bảo vệ dữ liệu trong suốt quá trình thiết kế, triển khai, vận hành hệ thống thông tin, nền tảng số, dịch vụ số; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật quốc gia về an toàn thông tin mạng, bảo vệ dữ liệu cá nhân; chịu trách nhiệm trước cơ quan chủ quản và cơ quan có thẩm quyền nếu để xảy ra sự cố, rò rỉ, mất an toàn thông tin do lỗi chủ quan hoặc vi phạm quy trình. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet trên địa bàn tỉnh phải phát huy vai trò là tuyến đầu phòng thủ và có trách nhiệm tuân thủ quy định trong công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu.		