

KẾ HOẠCH

Triển khai thực hiện Đề án “*Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng*” trên địa bàn tỉnh

Căn cứ Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ về việc phê duyệt Đề án “*Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia*”; Quyết định số 801/QĐ-BCĐ ngày 25/3/2026 của Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và Đề án 06 tỉnh Đồng Tháp về việc ban hành Chương trình công tác năm 2026 của Ban Chỉ đạo về phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và Đề án 06 tỉnh Đồng Tháp; Ủy ban nhân dân tỉnh ban hành Kế hoạch triển khai thực hiện Đề án “*Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng*” trên địa bàn tỉnh, với những nội dung như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Cụ thể hóa các quan điểm, mục tiêu, nhiệm vụ, giải pháp của Quyết định số 515/QĐ-TTg phù hợp với tình hình thực tiễn của tỉnh Đồng Tháp; xây dựng lực lượng bảo vệ an ninh mạng địa phương theo hướng cách mạng, chính quy, tinh nhuệ, hiện đại.

- Chủ động phòng ngừa, phát hiện, xử lý kịp thời các nguy cơ, hành vi xâm phạm an ninh mạng, bảo vệ dữ liệu quan trọng và an ninh chính trị trên địa bàn tỉnh.

2. Yêu cầu

- Triển khai quyết liệt, đồng bộ, hiệu quả, bảo đảm tính khả thi, phù hợp với nguồn lực của địa phương; gắn với các chương trình chuyển đổi số, phát triển khoa học công nghệ của tỉnh.

- Huy động sức mạnh tổng hợp của cả hệ thống chính trị, phối hợp chặt chẽ giữa các lực lượng bảo vệ an ninh mạng tại các cơ quan, đơn vị, địa phương, doanh nghiệp trên địa bàn tỉnh.

- Nâng cao năng lực tổng thể, xây dựng lực lượng bảo vệ an ninh mạng tinh nhuệ, hiện đại, nhằm chủ động phòng ngừa, sẵn sàng ứng phó hiệu quả với mọi nguy cơ, thách thức trên không gian mạng, bảo vệ vững chắc an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

3. Mục tiêu đến năm 2030

a) Triển khai kiến thức, kỹ năng chuyên sâu, chương trình, nội dung tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng; quản lý, hướng dẫn và tổ chức triển khai hoạt động chứng nhận tập huấn kiến thức, kỹ năng chuyên sâu về an ninh mạng.

b) 100% lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh; nhân sự trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4 trong cơ quan, tổ chức, doanh nghiệp nhà nước có chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng do cơ quan có thẩm quyền cấp; được cập nhật kiến thức an ninh mạng ít nhất 01 lần/năm.

c) 90% người sử dụng Internet có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an ninh mạng.

d) Thiết lập cơ chế chia sẻ thông tin, cảnh báo, điều phối ứng phó sự cố giữa các lực lượng bảo vệ an ninh mạng và các doanh nghiệp viễn thông, an ninh mạng để nâng cao năng lực phòng thủ quốc gia.

đ) 70% các cơ quan, đơn vị, địa phương sử dụng sản phẩm công nghệ chiến lược “Make in Vietnam”; 100% các sản phẩm, dịch vụ an ninh mạng phải được kiểm định, đánh giá trước khi đưa vào sử dụng, áp dụng trước hết đối với hạ tầng thông tin quan trọng của tỉnh, hệ thống thông tin của các cơ quan trong hệ thống chính trị có ảnh hưởng trực tiếp đến trật tự xã hội và đời sống nhân dân.

e) 100% hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh được triển khai đầy đủ các phương án bảo đảm an ninh mạng theo cấp độ;

g) 100% công chức, viên chức phụ trách công nghệ thông tin tại các sở, ban, ngành và Ủy ban nhân dân các xã, phường được tập huấn, bồi dưỡng và cấp chứng nhận về kỹ năng an ninh mạng chuyên sâu.

h) Hình thành mạng lưới ứng cứu sự cố an ninh mạng thống nhất từ tỉnh đến cơ sở.

i) Nghiên cứu, phát triển, từng bước làm chủ công nghệ chiến lược về an ninh mạng.

II. NHIỆM VỤ, GIẢI PHÁP

1. Hoàn thiện thể chế, xây dựng và triển khai các cơ chế, chính sách đặc thù

a) Rà soát, cập nhật, hoàn thiện các văn bản quy phạm pháp luật, văn bản hướng dẫn công tác bảo đảm an ninh mạng bảo đảm đồng bộ, thống nhất, hiệu quả giữa các lực lượng, đáp ứng yêu cầu quản lý, bảo vệ không gian mạng trong bối cảnh phát triển nhanh chóng của các công nghệ mới.

b) Tổ chức triển khai các nội dung của Công ước Liên Hợp quốc về chống tội phạm mạng theo chỉ đạo của Trung ương; điều chỉnh, bổ sung xây dựng các quy định thống nhất nhằm thực hiện các thủ tục và thực thi pháp luật phù hợp với quy định của Công ước; sẵn sàng các điều kiện cho việc thiết lập đường dây nóng 24/7 tham gia mạng lưới ứng cứu xử lý sự cố theo quy định của Công ước.

c) Triển khai các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật đối với các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, thiết lập cơ chế hợp chuẩn, hợp quy, đánh giá sự phù hợp, tổ chức đánh giá, công bố sản phẩm đáp ứng các tiêu chuẩn, quy chuẩn đã ban hành, 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 có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống nhân dân;

d) Triển khai khung quản lý rủi ro an ninh mạng quốc gia, chuyển đổi từ quản lý kỹ thuật thuần túy sang quản trị rủi ro toàn diện, dựa trên các tiêu chuẩn quốc tế nhằm tăng tính chủ động của các cơ quan, tổ chức trong việc phân bổ nguồn lực, giảm thiểu tổn thất từ các cuộc tấn công.

đ) Tiếp tục nghiên cứu, hoàn thiện, tổ chức triển khai có hiệu quả các cơ chế và chính sách ưu đãi nhằm thu hút, trọng dụng, bồi dưỡng, nâng cao chất lượng nguồn nhân lực cho lực lượng bảo vệ an ninh mạng của tỉnh.

2. Tổ chức lực lượng an ninh mạng

a) củng cố, kiện toàn Ban Chỉ đạo An ninh mạng tỉnh và các bộ phận thường trực tại các sở, ban, ngành.

b) củng cố, kiện toàn cơ quan chuyên trách về an ninh mạng tại Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh; hướng dẫn các sở, ban, ngành, Ủy ban nhân dân cấp xã,

cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia tổ chức lực lượng bảo vệ an ninh mạng.

c) Hình thành đội ngũ chuyên gia an ninh mạng có năng lực chuyên sâu về các công nghệ trọng yếu (AI, mật mã kháng lượng tử, blockchain,...), tiệm cận trình độ quốc tế.

3. Đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao

a) Triển khai khung tiêu chuẩn chức danh, vị trí việc làm, khung kiến thức, kỹ năng chuyên sâu về an ninh mạng; quy định về đào tạo, sát hạch, cấp chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng cho lực lượng bảo vệ an ninh mạng, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4 trong cơ quan, tổ chức, doanh nghiệp nhà nước.

b) Xây dựng, ban hành và định kỳ cập nhật các chương trình khung, tài liệu, giáo trình đào tạo tập huấn về bảo vệ an ninh mạng; chuẩn hóa hoạt động đào tạo, tập huấn đáp ứng yêu cầu về chuẩn kỹ năng và kiến thức về an ninh mạng tương ứng với từng cấp độ năng lực.

c) Hằng năm, trên cơ sở khảo sát nhu cầu thực tiễn, tổ chức các khóa đào tạo, tập huấn ngắn hạn theo hình thức tập trung, trực tuyến hoặc kết hợp cho các cơ quan của Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam tỉnh (gồm các tổ chức chính trị - xã hội) từ tỉnh đến cấp xã và lực lượng vũ trang để cập nhật kiến thức, huấn luyện chuyên sâu kiến thức, kỹ năng an ninh mạng. Nội dung đào tạo bao gồm:

- Đào tạo nghiệp vụ quản lý và kỹ năng bảo đảm an ninh mạng cho đội ngũ lãnh đạo, quản lý;

- Đào tạo kiến thức, kỹ năng bảo đảm an ninh mạng của người dùng cho các cán bộ công chức, viên chức và người lao động;

- Huấn luyện, đào tạo kỹ năng chuyên sâu cho lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, lực lượng bảo vệ an ninh mạng được bố trí tại sở, ban, ngành, Ủy ban nhân dân cấp xã, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4 trong cơ quan, tổ chức, doanh nghiệp nhà nước theo khung chương trình, yêu cầu kỹ năng do Bộ Công an ban hành, các chương trình đào tạo theo chứng chỉ quốc tế, lựa chọn nhân sự xuất

sắc tham gia thi chứng chỉ quốc tế. Định kỳ tổ chức bồi dưỡng, cập nhật bổ sung các kiến thức, kỹ năng theo các chuyên đề chuyên sâu về công nghệ mới.

d) Hàng năm tổ chức diễn tập thực chiến nhằm nâng cao năng lực ứng phó và phối hợp tác chiến trên không gian mạng.

đ) Đưa kiến thức 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; tổ chức cuộc thi, diễn đàn, câu lạc bộ an ninh mạng học đường và duy trì hoạt động hằng năm.

e) Phổ biến, nâng cao kiến thức an ninh mạng cho người dân qua các nền tảng học tập số, "Bình dân học vụ số", các khóa học trực tuyến đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng.

g) Xây dựng nền tảng quản lý hoạt động tập huấn, đánh giá và chứng nhận kiến thức, kỹ năng chuyên sâu về an ninh mạng; quản lý, xác thực dữ liệu các chứng chỉ an ninh mạng trong nước và quốc tế uy tín, quản lý các tổ chức đủ điều kiện thi, cấp, gia hạn, thu hồi chứng chỉ an ninh mạng phục vụ công nhận tương đương, hình thành và phát triển bản đồ chuyên gia an ninh mạng.

h) Phát triển nhân lực an ninh mạng, kết nối nhà trường/viện nghiên cứu (sinh viên, giảng viên, nghiên cứu viên), doanh nghiệp và cơ quan nhà nước trong lĩnh vực an ninh mạng, thúc đẩy liên kết công - tư và bồi dưỡng thế hệ chuyên gia an ninh mạng mới.

4. Giám sát, chia sẻ thông tin và đánh giá năng lực an ninh mạng quốc gia

a) Xây dựng bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng đối với cơ quan tổ chức, doanh nghiệp.

b) Triển khai hệ thống chia sẻ thông tin tình báo an ninh mạng (Threat Intelligence), hướng tới hình thành các trung tâm phân tích và chia sẻ thông tin an ninh mạng (ISAC - Information Sharing Analysis Center) cho từng ngành, lĩnh vực trọng yếu (tài chính, ngân hàng, giao thông, năng lượng,...), thúc đẩy cơ chế chia sẻ thông tin tình báo về các mối đe dọa, lỗ hổng bảo mật và các cuộc tấn công an ninh mạng giữa khu vực công và tư nhân, đảm bảo tính đồng bộ, hiệu quả và bảo mật.

c) Triển khai nền tảng giám sát, điều hành an ninh mạng quốc gia cho phép báo cáo, thống kê, cập nhật dữ liệu an ninh mạng trên toàn quốc, đảm bảo dữ liệu "đúng, đủ, sạch, sống, dùng chung, thống nhất".

5. Nghiên cứu phát triển, nâng cao năng lực tự chủ công nghệ, làm chủ công nghệ lõi trong lĩnh vực an ninh mạng

a) Rà soát, xây dựng, công bố danh mục công nghệ, danh mục sản phẩm, dịch vụ an ninh mạng cốt lõi, ưu tiên làm chủ, tự chủ.

b) Thúc đẩy cơ chế đề cơ quan nhà nước đặt hàng doanh nghiệp phát triển các sản phẩm về an ninh mạng; ưu tiên thí điểm, thử nghiệm các sản phẩm do Việt Nam làm chủ công nghệ, gồm:

- Khuyến khích nghiên cứu, phát triển các sản phẩm, dịch vụ an ninh mạng nội địa theo hướng hỗ trợ đầu ra, tạo thị trường cho doanh nghiệp. Tổ chức các cuộc thi, giải thưởng cấp tỉnh nhằm tìm kiếm, đánh giá và công nhận các sản phẩm, dịch vụ an ninh mạng xuất sắc, chất lượng cao của các doanh nghiệp Việt Nam;

- Triển khai các giải pháp hỗ trợ các doanh nghiệp khởi nghiệp sáng tạo về an ninh mạng thông qua việc cung cấp các ưu đãi, hỗ trợ các doanh nghiệp trong nước chuyên về nghiên cứu và phát triển sản phẩm, dịch vụ an ninh mạng.

- Triển khai các giải pháp hỗ trợ các doanh nghiệp vừa và nhỏ bảo đảm an ninh mạng thông qua các gói hỗ trợ đào tạo, tư vấn, cung cấp giải pháp an ninh mạng nội địa.

c) Nghiên cứu, kiện toàn và phát triển đơn vị nòng cốt trong lĩnh vực đổi mới sáng tạo và huấn luyện an ninh mạng thuộc Công an tỉnh, làm trung tâm kết nối và phát triển hệ sinh thái an ninh mạng; thực hiện chức năng định hướng chiến lược, xác định ưu tiên phát triển, kết nối và điều phối các nguồn lực, hỗ trợ nghiên cứu, đề xuất hoàn thiện chính sách và pháp luật thúc đẩy phát triển ngành công nghiệp an ninh mạng, đồng thời tổ chức đào tạo, huấn luyện bồi dưỡng chuyên sâu về an ninh mạng.

d) Tăng cường phối hợp công tư, xây dựng và vận hành có hiệu quả tam giác chiến lược Nhà nước - Nhà trường (Viện nghiên cứu) - Doanh nghiệp trong việc định hướng, nghiên cứu, nắm bắt các công nghệ lõi, công nghệ chiến lược, phát triển, triển khai các công nghệ, sản phẩm, dịch vụ an ninh mạng.

6. Nâng cao uy tín quốc gia và tăng cường hợp tác quốc tế

a) Tăng cường hợp tác với các tỉnh có thế mạnh, phát triển về an ninh mạng, các tổ chức lớn thông qua các hoạt động chia sẻ thông tin, hỗ trợ kỹ thuật, và đào tạo nhân lực.

b) Thu hút nguồn lực từ nước ngoài và các đối tác quốc tế cho hoạt động nghiên cứu, ứng dụng, đổi mới sáng tạo, khởi nghiệp, chuyển giao công nghệ về bảo đảm an ninh mạng.

c) Đưa chuyên gia, tổ chức trong tỉnh tham gia các hoạt động toàn cầu, các hội nghị như: RSAC Conference, Black Hat, DEFCON, CyberTech, Hack in the Box...; khuyến khích doanh nghiệp, viện nghiên cứu đạt các chứng nhận, giải thưởng quốc tế về an ninh mạng.

7. Kinh phí thực hiện

Nguồn ngân sách nhà nước; nguồn của các doanh nghiệp, tổ chức để triển khai các hoạt động nâng cao năng lực tại đơn vị; các nguồn hợp pháp khác theo quy định.

III. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh

a) Giúp Ủy ban nhân dân tỉnh triển khai các hoạt động nâng cao năng lực các lực lượng bảo vệ an ninh mạng.

b) Rà soát, đề xuất sửa đổi, bổ sung theo thẩm quyền hoặc kiến nghị cơ quan có thẩm quyền sửa đổi, bổ sung, hoàn thiện, chính sách pháp luật về an ninh mạng, tổ chức lực lượng an ninh mạng.

c) Chủ trì, phối hợp với Sở Giáo dục và Đào tạo, Sở Nội vụ và các sở, ban, ngành có liên quan triển khai các nhiệm vụ phát triển nguồn nhân lực an ninh mạng của tỉnh.

d) Chủ trì triển khai các giải pháp giám sát, chia sẻ thông tin và đánh giá năng lực an ninh mạng, triển khai các chương trình, thúc đẩy hoạt động nghiên cứu phát triển, nâng cao năng lực tự chủ công nghệ, đặc biệt chú trọng làm chủ các công nghệ lõi trong lĩnh vực an ninh mạng.

đ) Định kỳ sơ kết, tổng kết, đánh giá tình hình thực hiện Đề án, đề xuất Ủy ban nhân dân tỉnh, Bộ Công an sửa đổi, bổ sung cho phù hợp với tình hình thực tế.

e) Hàng năm tổ chức ít nhất 01 cuộc diễn tập chuyên đề an ninh mạng, ứng cứu sự cố mạng trong phạm vi của bộ, ngành, địa phương mình; phối hợp, tham gia các cuộc diễn tập quốc gia và quốc tế do Bộ Công an tổ chức.

g) Hàng năm tổ chức các khóa đào tạo, tập huấn trực tiếp hoặc trực tuyến nhằm

cập nhật, nâng cao năng lực, kiến thức, kỹ năng cho cán bộ các cấp (gồm quản lý, lãnh đạo; người dùng cuối; nhân sự kỹ thuật an ninh mạng) theo hướng dẫn Bộ Công an, khuyến khích thi lấy chứng chỉ quốc tế.

2. Sở Khoa học và Công nghệ

Chủ trì, đề xuất phương án dự toán chi ngân sách nhà nước cho các nhiệm vụ, dự án phù hợp với ngành, lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số của các sở, ban, ngành và địa phương để triển khai Đề án Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia theo pháp luật về ngân sách nhà nước, đầu tư công, khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số và pháp luật liên quan, gửi Sở Tài chính tổng hợp, trình Ủy ban nhân dân tỉnh quyết định.

3. Sở Giáo dục và Đào tạo

a) Nghiên cứu, tổng hợp đề xuất của các cơ quan liên quan, báo cáo cấp có thẩm quyền xem xét sửa đổi, bổ sung các chính sách ưu đãi, miễn giảm học phí, học bổng cho học sinh, sinh viên nhằm thu hút nguồn nhân lực và đào tạo nguồn nhân lực ngành an ninh mạng.

b) Chủ trì, phối hợp với Công an tỉnh, Sở Tài chính nghiên cứu, đề xuất và tổ chức triển khai mô hình liên kết giữa nhà nước, nhà trường, doanh nghiệp trong đào tạo nguồn nhân lực ngành an ninh mạng.

4. Sở Nội vụ

Phối hợp với Công an tỉnh trong xây dựng tiêu chuẩn chuyên môn, nghiệp vụ cho lực lượng bảo vệ an ninh mạng, đề xuất cơ chế thu hút nhân lực chất lượng cao làm việc trong lĩnh vực an ninh mạng, cơ chế giữ chân nhân lực an ninh mạng làm việc tại cơ quan nhà nước.

5. Sở Tài chính

a) Cân đối nguồn ngân sách nhà nước hằng năm cho lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số theo quy định của pháp luật về ngân sách, về đầu tư công và pháp luật quản lý ngành, lĩnh vực. Tổng hợp, trình cấp có thẩm quyền xem xét, quyết định trên cơ sở đề xuất của Sở Khoa học và Công nghệ về dự toán chi ngân sách nhà nước cho lĩnh vực khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số.

b) Phối hợp với Công an tỉnh tranh thủ các nguồn kinh phí Trung ương hỗ trợ cho các hoạt động nghiên cứu, ứng dụng, đổi mới sáng tạo, khởi nghiệp, chuyển giao công nghệ về bảo đảm an ninh mạng theo quy định của pháp luật.

6. Bộ Chỉ huy Quân sự tỉnh

a) Triển khai đồng bộ, hiệu quả các giải pháp bảo đảm an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý.

b) Chỉ đạo các cơ quan, tổ chức, nghiên cứu, phát triển các sản phẩm an ninh mạng theo hướng lưỡng dụng, tập trung vào các sản phẩm công nghệ chiến lược "Make in Vietnam" thuộc phạm vi quản lý.

c) Tăng cường triển khai các giải pháp giám sát, bảo đảm an ninh mạng đối với các hệ thống thông tin quan trọng quốc gia theo chức trách, nhiệm vụ được giao.

d) Rà soát, hoàn thiện mô hình tổ chức lực lượng chuyên trách bảo vệ an ninh mạng thuộc phạm vi quản lý.

đ) Tổ chức tập huấn và chứng nhận kiến thức, kỹ năng chuyên sâu về an ninh mạng cho các đối tượng thuộc phạm vi quản lý.

e) Nghiên cứu hướng dẫn hoạt động đăng ký, chỉ định và quản lý hoạt động của tổ chức chứng nhận sự phù hợp về an ninh mạng trong phạm vi quản lý.

g) Phối hợp chặt chẽ với Công an tỉnh trong triển khai các nhiệm vụ, giải pháp, đặc biệt là phát triển nguồn nhân lực, tổ chức diễn tập; giám sát, chia sẻ thông tin và đánh giá năng lực an ninh mạng quốc gia.

7. Các sở, ban, ngành và Ủy ban nhân dân các xã, phường

a) Ưu tiên bố trí nguồn lực (nhân lực, kinh phí) và điều kiện để triển khai hoạt động bảo đảm an ninh mạng trong hoạt động nội bộ của cơ quan, tổ chức và lĩnh vực quản lý.

b) Hàng năm phân công lực lượng tham gia diễn tập chuyên đề an ninh mạng, ứng cứu sự cố mạng trong phạm vi của đơn vị, địa phương mình; phối hợp, tham gia các cuộc diễn tập quốc gia và quốc tế do Bộ Công an tổ chức.

c) Tham gia các khóa đào tạo, tập huấn trực tiếp hoặc trực tuyến nhằm cập nhật, nâng cao năng lực, kiến thức, kỹ năng cho cán bộ các cấp (gồm quản lý, lãnh đạo; người dùng cuối; nhân sự kỹ thuật an ninh mạng) theo hướng dẫn Bộ Công an,

khuyến khích thi lấy chứng chỉ quốc tế.

d) Trang bị hệ thống, công cụ chuyên dụng cho lực lượng bảo vệ an ninh mạng, tối thiểu gồm: hệ thống, công cụ rà quét phát hiện lỗ hổng bảo mật; hệ thống, công cụ hỗ trợ điều tra số, ứng cứu, khắc phục sự cố an ninh mạng.

đ) Đẩy mạnh hoạt động bảo đảm an ninh mạng trong phạm vi quản lý; tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn nghiệp vụ của Bộ Công an và quy định của pháp luật; ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng “Make in Vietnam”. Gắn kết công tác bảo đảm an ninh mạng với công tác triển khai chuyển đổi số, ứng dụng công nghệ thông tin, phát triển chính quyền số, kinh tế số, xã hội số và phát triển đô thị thông minh.

Trong quá trình thực hiện, nếu phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương kịp thời báo cáo, đề xuất Ủy ban nhân dân tỉnh (qua Công an tỉnh) để xem xét, điều chỉnh phù hợp./.

Nơi nhận:

- Thường trực Tỉnh ủy;
- Chủ tịch và các PCT UBND tỉnh;
- Như Mục III;
- VPUB: CVP, các PCVP;
- Lưu: VT, KGVX(vttoan).

**TM. ỦY BAN NHÂN DÂN
KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**



Huỳnh Minh Tuấn

Phụ lục
DANH MỤC CÁC NHIỆM VỤ, GIẢI PHÁP TRIỂN KHAI THỰC HIỆN
(Kèm theo Kế hoạch số /KH-UBND ngày tháng năm 2026 của Ủy ban nhân dân tỉnh)

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
I. HOÀN THIỆN HÀNH LANG PHÁP LÝ, ĐẨY MẠNH TRIỂN KHAI CÁC CƠ CHẾ, CHÍNH SÁCH				
1	Rà soát, cập nhật, hoàn thiện hành lang pháp lý, văn bản hướng dẫn công tác bảo đảm an ninh mạng theo thẩm quyền.	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã	Thường xuyên
2	Tham mưu trình UBND tỉnh Kế hoạch triển khai thi hành Luật An ninh dữ liệu	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã	Khi Luật ban hành
3	Tham mưu xây dựng, trình UBND triển khai Nghị định, văn bản hướng dẫn thi hành Luật An ninh mạng gồm: Nghị định quy định chi tiết một số điều Luật An ninh mạng, Nghị định về bảo vệ an ninh hệ thống thông tin theo cấp độ, Nghị định về ngăn chặn xung đột thông tin trên mạng, Nghị định quy định điều kiện kinh doanh sản phẩm, dịch vụ an ninh mạng, Nghị định kinh doanh sản phẩm, dịch vụ mật mã dân sự, xuất khẩu, nhập khẩu sản phẩm mật mã dân sự, Nghị định quy định biện pháp bảo đảm an ninh mạng.	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã	Quý II/2026
4	Triển khai Công ước Liên Hợp quốc về chống tội phạm mạng.	Công an tỉnh	Sở Tư pháp	Quý IV/2026
5	Rà soát, đề xuất hoàn chỉnh hành lang pháp lý về công tác phòng chống tội phạm mạng theo khuyến nghị của Công ước; điều chỉnh, bổ sung xây dựng các quy định thống nhất nhằm thực hiện các biện pháp thủ tục và thực thi pháp luật phù hợp với quy định của Công ước; sẵn sàng các điều kiện cho việc xây dựng lực lượng tham gia mạng lưới 24/7 theo quy định của Công ước.	Công an tỉnh , Sở Tư pháp	Các sở, ban, ngành, UBND cấp xã	2026 - 2027

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
6	Rà soát sửa đổi TCVN 14423:2025 trên cơ sở hợp nhất TCVN 14423:2025 và TCVN 11930:2017 cho phù hợp với các cấp độ hệ thống thông tin theo Luật An ninh mạng 116/2025/QH15.	Công an tỉnh	Sở Khoa học và Công nghệ	Quý II/2026
7	Triển khai Khung quản lý rủi ro an ninh mạng quốc gia, ban hành hướng dẫn về quản lý rủi ro an ninh mạng để các đơn vị, địa phương nghiên cứu, chuẩn bị nguồn lực thực hiện.	Công an tỉnh	Sở Khoa học và Công nghệ, Bộ Chỉ huy Quân sự tỉnh	Quý IV/2026
8	Rà soát, đề xuất chính sách ưu đãi cho doanh nghiệp nghiên cứu phát triển sản phẩm an ninh mạng trên địa bàn tỉnh.	Sở Tài chính, Công an tỉnh	Các sở, ban, ngành	2026 - 2027
II. TỔ CHỨC LỰC LƯỢNG AN NINH MẠNG				
9	Rà soát, hướng dẫn xây dựng mô hình tổ chức lực lượng bảo vệ an ninh mạng tại sở, ban, ngành, địa phương, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia.	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã	Quý IV/2026
III. PHÁT TRIỂN NGUỒN NHÂN LỰC AN NINH MẠNG CHẤT LƯỢNG CAO				
10	Triển khai khung kiến thức, kỹ năng chuyên sâu về an ninh mạng; quy định về chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng cho lực lượng bảo vệ an ninh mạng, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4 trong cơ quan, tổ chức, doanh nghiệp nhà nước.	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã	2026 - 2027 (khi Trung ương ban hành)
11	Tổ chức các chương trình diễn tập, chương trình đào tạo, huấn luyện, bồi dưỡng về an ninh mạng nhằm nâng cao năng lực, kiến thức, kỹ năng cho cán bộ các cấp gồm quản lý, lãnh đạo; cán bộ, công chức; nhân sự kỹ thuật an ninh mạng, các chương trình đào tạo, thi lấy chứng chỉ quốc tế.	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã, các tổ chức, doanh nghiệp nhà nước	Hàng năm
12	Tổ chức diễn tập chuyên đề an ninh mạng, ứng cứu sự cố mạng trong phạm vi quản lý, tổ chức các khóa đào tạo, tập huấn trực tiếp hoặc trực tuyến nhằm cập nhật, nâng cao năng lực, kiến thức, kỹ	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã, các tổ	Hàng năm

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
	năng cho cán bộ các cấp (gồm quản lý, lãnh đạo; người dùng cuối; nhân sự kỹ thuật an ninh mạng) theo hướng dẫn Bộ Công an, khuyến khích thi lấy chứng chỉ quốc tế.		chức, doanh nghiệp nhà nước	
13	Phổ biến, nâng cao kiến thức an ninh mạng cho người dân qua các nền tảng học tập số, "Bình dân học vụ số", các khóa học trực tuyến đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng.	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã, các tổ chức, doanh nghiệp nhà nước	Hàng năm
IV. GIẢI PHÁP GIÁM SÁT, CHIA SẺ THÔNG TIN VÀ ĐÁNH GIÁ NĂNG LỰC AN NINH MẠNG QUỐC GIA				
14	Triển khai chỉ số đảm bảo an ninh mạng để đánh giá năng lực bảo đảm an ninh mạng của các cơ quan tổ chức, doanh nghiệp.	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã	2026 - 2027 (khi Trung ương ban hành)
15	Triển khai hệ thống chia sẻ thông tin tình báo an ninh mạng (Threat Intelligence), hướng tới hình thành các trung tâm phân tích và chia sẻ thông tin an ninh mạng (ISAC - Information Sharing Analysis Center) cho từng ngành, lĩnh vực trọng yếu (tài chính, ngân hàng, giao thông, năng lượng,...), thúc đẩy cơ chế chia sẻ thông tin tình báo về các mối đe dọa, lỗ hổng bảo mật và các cuộc tấn công an ninh mạng giữa khu vực công và tư nhân, đảm bảo tính đồng bộ, hiệu quả và bảo mật.	Công an tỉnh, sở Khoa học và Công nghệ	Các sở, ban, ngành, UBND cấp xã, các doanh nghiệp tham gia bảo vệ an ninh mạng	2026 - 2028 (khi Trung ương ban hành)
16	Triển khai nền tảng theo dõi, điều hành an ninh mạng quốc gia cho phép báo cáo, thống kê, cập nhật dữ liệu an ninh mạng trên toàn quốc, đảm bảo dữ liệu "đúng, đủ, sạch, sống, dùng chung, thống nhất".	Công an tỉnh	Các sở, ban, ngành, UBND cấp xã	2026 - 2027 (khi Trung ương ban hành)
17	Trang bị hệ thống, công cụ chuyên dụng cho các lực lượng bảo vệ an ninh mạng, tối thiểu gồm hệ thống, công cụ rà quét phát hiện lỗ	Các sở, ban, ngành, UBND cấp xã	Công an tỉnh	Thường xuyên

STT	Nhiệm vụ, giải pháp	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian triển khai
	hồng bảo mật; hệ thống, công cụ hỗ trợ điều tra số, ứng cứu, khắc phục sự cố an ninh mạng.			
V. NGHIÊN CỨU PHÁT TRIỂN, NÂNG CAO NĂNG LỰC TỰ CHỦ CÔNG NGHỆ, ĐẶC BIỆT CHÚ TRỌNG LÀM CHỦ CÁC CÔNG NGHỆ LỖI TRONG LĨNH VỰC AN NINH MẠNG				
18	Xây dựng và triển khai các chương trình, thúc đẩy cơ chế để cơ quan nhà nước đặt hàng doanh nghiệp phát triển các sản phẩm về an ninh mạng; ưu tiên thí điểm, thử nghiệm các sản phẩm do Việt Nam làm chủ công nghệ.	Công an tỉnh, Sở Khoa học và Công nghệ	Sở Tài chính, các cơ quan, doanh nghiệp và hội, hiệp hội trong lĩnh vực an ninh mạng, công nghệ thông tin - truyền thông	Khi Trung ương ban hành hướng dẫn
19	Tăng cường phối hợp công tư, xây dựng và vận hành có hiệu quả tam giác chiến lược Nhà nước - Nhà trường (Viện nghiên cứu) - Doanh nghiệp trong việc định hướng, nghiên cứu, nắm bắt các công nghệ lõi, công nghệ chiến lược, phát triển, triển khai các công nghệ, sản phẩm, dịch vụ an ninh mạng.	Sở Khoa học và Công nghệ, Sở Giáo dục và Đào tạo, Công an tỉnh	Các cơ quan, doanh nghiệp và hội, hiệp hội trong lĩnh vực an ninh mạng, CNTT-TT	Khi Trung ương ban hành hướng dẫn