ỦY BAN NHÂN DÂN TỈNH GIA LAI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 310 /KH-UBND	*Gia Lai, ngày 04 tháng 8 năm 2026*

KẾ HOẠCH
Triển khai Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ về Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia" trên địa bàn tỉnh Gia Lai

Căn cứ Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ phê duyệt Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia";

Theo đề nghị của Công an tỉnh tại Tờ trình số 8936/TTr-CAT-PC06 ngày 30/7/2026, Ủy ban nhân dân tỉnh ban hành Kế hoạch triển khai Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ về Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia" trên địa bàn tỉnh Gia Lai, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Cụ thể hóa và triển khai thực hiện hiệu quả Quyết định số 515/QĐ-TTg ngày 30/3/2026 của Thủ tướng Chính phủ phê duyệt Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia" (sau đây gọi tắt là Đề án) trên địa bàn tỉnh Gia Lai.

- Nâng cao năng lực tổng thể của lực lượng bảo vệ an ninh mạng trên địa bàn tỉnh; chủ động phòng ngừa, phát hiện, ứng phó và xử lý hiệu quả các nguy cơ, sự cố an ninh mạng, góp phần bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội và quyền, lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

2. Yêu cầu

- Việc triển khai phải bám sát mục tiêu, nhiệm vụ, giải pháp và lộ trình tại Quyết định số 515/QĐ-TTg; phù hợp chức năng, thẩm quyền, điều kiện thực tế của tỉnh; bảo đảm đồng bộ, thiết thực, hiệu quả, tránh hình thức, chồng chéo và lãng phí nguồn lực.

- Phân công rõ cơ quan chủ trì, cơ quan phối hợp, thời gian thực hiện và sản phẩm đầu ra; gắn trách nhiệm người đứng đầu với tiến độ, chất lượng thực hiện nhiệm vụ.

- Kết hợp chặt chẽ giữa kiện toàn lực lượng, đào tạo nhân lực, đầu tư công cụ kỹ thuật, giám sát, cảnh báo, ứng phó sự cố và nâng cao nhận thức; ưu tiên bảo

vệ hệ thống thông tin quan trọng, hệ thống thông tin cấp độ 3 trở lên và hệ thống phục vụ chỉ đạo, điều hành, cung cấp dịch vụ công của tỉnh.

- Bảo đảm sự phối hợp thống nhất giữa lực lượng chuyên trách bảo vệ an ninh mạng, cơ quan quản lý nhà nước về an toàn thông tin, cơ quan chủ quản hệ thống thông tin, doanh nghiệp và các đơn vị liên quan; chủ động kết nối, chia sẻ thông tin với các nền tảng, hệ thống của Trung ương theo hướng dẫn của Bộ Công an.

II. MỤC TIÊU

1. Mục tiêu chung

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.

2. Mục tiêu cụ thể

a) Mục tiêu đến năm 2030

- 100% lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại cơ quan, đơn vị trên địa bàn tỉnh 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, cấp độ 5 phải có chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng do cơ quan có thẩm quyền cấp.

- Rà soát, ban hành hoặc tham mưu cấp có thẩm quyền ban hành các văn bản thuộc phạm vi quản lý của tỉnh; thiết lập cơ chế trao đổi, chia sẻ thông tin, cảnh báo và phối hợp ứng phó sự cố giữa các cơ quan, đơn vị, địa phương và doanh nghiệp có liên quan.

- Phấn đấu đạt tỷ lệ tối thiểu 70% cơ quan, đơn vị thuộc phạm vi quản lý của UBND tỉnh và các hệ thống thông tin trọng yếu của tỉnh ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng 'Make in Vietnam' đáp ứng tiêu chuẩn, quy chuẩn và yêu cầu kỹ thuật theo quy định.

- 100% sản phẩm, giải pháp, dịch vụ an ninh mạng được đầu tư, mua sắm hoặc thuê để sử dụng trong các hệ thống thông tin của cơ quan nhà nước trên địa bàn tỉnh thuộc diện phải kiểm định, đánh giá, chứng nhận theo quy định được thực hiện kiểm định, đánh giá trước khi đưa vào sử dụng.

- 100% các hệ thống thông tin sử dụng vốn ngân sách nhà nước được triển khai đầy đủ các phương án bảo đảm an ninh mạng theo đúng cấp độ.

- 90% người sử dụng Internet trên địa bàn tỉnh có cơ hội tiếp cận các hoạt động tuyên truyền, đào tạo, hướng dẫn kỹ năng và công cụ bảo đảm an ninh mạng.

b) Tầm nhìn đến năm 2045

- Xây dựng lực lượng bảo vệ an ninh mạng tỉnh Gia Lai chính quy, tinh nhuệ, hiện đại; góp phần cùng cả nước đưa Việt Nam trở thành quốc gia dẫn đầu khu vực về an ninh mạng.

- Nâng cao năng lực phòng thủ, chủ động phòng ngừa, phát hiện, phối hợp đấu tranh, ngăn chặn, xử lý tội phạm mạng và các hoạt động xâm phạm an ninh quốc gia trên không gian mạng theo chức năng, thẩm quyền; bảo vệ vững chắc chủ quyền số và các hệ thống thông tin thuộc phạm vi quản lý của tỉnh.

- Bảo đảm môi trường mạng an toàn, tin cậy cho mọi hoạt động của các cơ quan Đảng, Nhà nước, doanh nghiệp và người dân trên địa bàn tỉnh, phục vụ đắc lực cho sự nghiệp phát triển kinh tế - xã hội bền vững của tỉnh.

III. NHIỆM VỤ, GIẢI PHÁP

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

- Rà soát các quy chế, quy định, quy trình thuộc phạm vi quản lý của tỉnh; ban hành, sửa đổi, bổ sung theo thẩm quyền hoặc kiến nghị cấp có thẩm quyền hoàn thiện các văn bản về bảo đảm an ninh mạng, bảo đảm sự phối hợp thống nhất giữa các lực lượng.

- Tổ chức triển khai Khung quản lý rủi ro an ninh mạng quốc gia và hướng dẫn của Bộ Công an; rà soát, đánh giá rủi ro, xác định mức độ ưu tiên và phương án phân bổ nguồn lực bảo vệ các hệ thống thông tin thuộc phạm vi quản lý của tỉnh.

- Hoàn thiện và tổ chức triển khai có hiệu quả cơ chế, 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 tỉnh.

2. Tổ chức lực lượng an ninh mạng

- Kiện toàn Tiểu Ban An ninh mạng tỉnh.

- Rà soát, kiện toàn lực lượng bảo vệ an ninh mạng tại cấp tỉnh và tại các cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia; phân công cán bộ hoặc đầu mối phụ trách công tác bảo đảm an ninh mạng tại các sở, ban, ngành và UBND cấp xã phù hợp với quy mô hệ thống, vị trí việc làm và điều kiện thực tế.

- Hoàn thiện các cơ chế trao đổi, chia sẻ thông tin, đồng thời xây dựng quy trình phối hợp giữa Công an tỉnh, Sở Khoa học và Công nghệ, cơ quan chủ quản hệ thống thông tin, các sở, ban, ngành, địa phương, doanh nghiệp và các đơn vị có liên quan trong trao đổi thông tin, cảnh báo, ứng phó và khắc phục sự cố an ninh mạng.

- Hình thành, phát triển mạng lưới chuyên gia có năng lực chuyên sâu về các công nghệ trọng yếu, công nghệ mới như trí tuệ nhân tạo, mật mã kháng lượng tử, blockchain và các công nghệ khác theo định hướng, hướng dẫn của Bộ Công an.

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

- Hàng năm, tổ chức các khóa đào tạo, tập huấn (trực tiếp hoặc trực tuyến) dựa trên việc khảo sát nhu cầu thực tiễn để cập nhật kiến thức, huấn luyện kỹ năng an ninh mạng cho đội ngũ lãnh đạo quản lý, cán bộ công chức, viên chức và người lao động.

- Tạo điều kiện để lực lượng chuyên trách bảo vệ an ninh mạng tỉnh được huấn luyện, đào tạo kỹ năng chuyên sâu theo khung chương trình, yêu cầu kỹ năng do Bộ Công an ban hành.

- Đồng hành, tham gia các chương trình diễn tập cấp quốc gia, chương trình diễn tập theo vùng nhằm nâng cao năng lực ứng phó và phối hợp tác chiến mạng.

- 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 đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng hàng năm.

- Bố trí nguồn nhân lực, kinh phí và các điều kiện cần thiết khác, nhằm bảo đảm triển khai hiệu quả công tác đào tạo, phát triển nguồn nhân lực phục vụ hoạt động bảo vệ an ninh mạng trên địa bàn tỉnh.

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

- Nghiên cứu và chuẩn bị các điều kiện cần thiết để triển khai Bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng đối với cơ quan, tổ chức, doanh nghiệp khi được Trung ương ban hành.

- Chuẩn bị các điều kiện kỹ thuật, tổ chức kết nối, cập nhật, báo cáo và chia sẻ dữ liệu với nền tảng giám sát, điều hành an ninh mạng quốc gia theo hướng dẫn của Bộ Công an; bảo đảm dữ liệu 'đúng, đủ, sạch, sống, dùng chung, thống nhất'.

- Phối hợp xây dựng hệ thống chia sẻ thông tin tình báo an ninh mạng. Hướng tới hình thành các trung tâm phân tích và chia sẻ thông tin cho các lĩnh vực trọng yếu, nhằm thúc đẩy việc chia sẻ thông tin về các mối đe dọa, lỗ hổng bảo mật và các cuộc tấn công giữa khu vực công và tư nhân.

5. Nguồn lực bảo đảm thực hiện

Nguồn ngân sách nhà nước; nguồn của các doanh nghiệp, tổ chức để triển khai các hoạt động nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng tại địa phương; các nguồn hợp pháp khác theo quy định.

IV. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh

- Cơ quan đầu mối, chủ trì tham mưu Ủy ban nhân dân tỉnh tổ chức triển khai thực hiện Kế hoạch này. Triển khai các hoạt động nâng cao năng lực các lực lượng bảo vệ an ninh mạng tại địa phương. Hằng năm, tổ chức ít nhất 01 cuộc

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 năng cho cán bộ các cấp (gồm: lãnh đạo, quản lý; người dùng cuối; nhân sự kỹ thuật an ninh mạng) theo hướng dẫn của Bộ Công an, khuyến khích thi lấy chứng chỉ quốc tế. Phối hợp, tham gia các cuộc diễn tập quốc gia và quốc tế do Bộ Công an tổ chức.

- Chủ động nghiên cứu, đề xuất các giải pháp, nội dung trọng tâm, bảo đảm việc triển khai đồng bộ, thống nhất và hiệu quả trên toàn địa bàn tỉnh. Tổ chức hướng dẫn, kiểm tra, đôn đốc các sở, ban, ngành, địa phương và các cơ quan, đơn vị liên quan trong quá trình thực hiện; kịp thời phát hiện khó khăn, vướng mắc để tham mưu Ủy ban nhân dân tỉnh chỉ đạo xử lý. Thực hiện tổng hợp tình hình, kết quả triển khai; định kỳ hoặc đột xuất báo cáo Ủy ban nhân dân tỉnh và các cơ quan có thẩm quyền theo quy định.

- Triển khai các giải pháp giám sát an ninh mạng, thu thập, phân tích, chia sẻ thông tin, cảnh báo sớm các nguy cơ, sự cố an ninh mạng; đồng thời tổ chức đánh giá năng lực bảo đảm an ninh mạng đối với các cơ quan, tổ chức, doanh nghiệp trên địa bàn theo hướng dẫn của cơ quan có thẩm quyền.

- Xây dựng, củng cố và phát triển lực lượng bảo vệ an ninh mạng tại địa phương theo hướng chuyên trách, tinh nhuệ, hiện đại.

2. Sở Khoa học và Công nghệ

- Phối hợp với các cơ quan, đơn vị liên quan triển khai các giải pháp bảo đảm an toàn thông tin, góp phần phát triển hạ tầng số của tỉnh theo hướng an toàn, tin cậy, bền vững; lồng ghép yêu cầu bảo đảm an ninh mạng trong các chương trình, nhiệm vụ khoa học và công nghệ trên địa bàn.

- Tham mưu Ủy ban nhân dân tỉnh thúc đẩy nghiên cứu, phát triển, ứng dụng và ưu tiên sử dụng các sản phẩm, giải pháp an ninh mạng "Make in Vietnam"; đồng thời tăng cường hỗ trợ doanh nghiệp đổi mới sáng tạo, làm chủ công nghệ, phát triển các sản phẩm, dịch vụ an ninh mạng trong nước, từng bước nâng cao năng lực tự chủ về công nghệ.

- Chủ trì, phối hợp thúc đẩy hoạt động nghiên cứu, ứng dụng, chuyển giao công nghệ trong lĩnh vực an ninh mạng; kết nối hệ sinh thái đổi mới sáng tạo, hỗ trợ các tổ chức, doanh nghiệp tham gia các chương trình, đề tài, dự án khoa học và công nghệ liên quan đến an ninh mạng.

3. Sở Giáo dục và Đào tạo

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan tổ chức lồng ghép nội dung đào tạo, bồi dưỡng kiến thức, kỹ năng về an ninh mạng, an toàn thông tin trong các chương trình giáo dục phổ thông phù hợp với từng cấp học; đồng thời

định hướng, phối hợp với các cơ sở giáo dục đại học, cơ sở đào tạo trên địa bàn tích hợp, phát triển các chương trình đào tạo liên quan đến lĩnh vực an ninh mạng.

- Phối hợp với Công an tỉnh, các sở, ngành và cơ sở đào tạo tổ chức đào tạo, bồi dưỡng, phát triển nguồn nhân lực an ninh mạng chất lượng cao phục vụ nhu cầu của địa phương; tăng cường các hoạt động tuyên truyền, nâng cao nhận thức, kỹ năng sử dụng không gian mạng an toàn cho học sinh, sinh viên.

- Khuyến khích các cơ sở giáo dục triển khai các hoạt động ngoại khóa, cuộc thi, câu lạc bộ về an toàn thông tin, an ninh mạng; từng bước hình thành nguồn nhân lực có kiến thức, kỹ năng cơ bản, đáp ứng yêu cầu trong tình hình mới.

4. Sở Tài chính

Căn cứ khả năng cân đối của ngân sách nhà nước và phân cấp ngân sách hiện hành; trên cơ sở đề nghị của các sở, ngành, địa phương có liên quan tham mưu cấp thẩm quyền trong việc bố trí nguồn kinh phí để thực hiện nội dung trong Kế hoạch theo quy định Luật Ngân sách nhà nước, Luật Đầu tư công và các văn bản hướng dẫn có liên quan.

5. Sở Nội vụ

- Chủ trì, phối hợp với các cơ quan, đơn vị liên quan nghiên cứu, tham mưu Ủy ban nhân dân tỉnh xây dựng, hoàn thiện cơ chế, chính sách phát triển nguồn nhân lực trong lĩnh vực an ninh mạng, bảo đảm phù hợp với yêu cầu nhiệm vụ và định hướng phát triển của địa phương.

- Tham mưu Ủy ban nhân dân tỉnh bố trí, sắp xếp, kiện toàn tổ chức bộ máy và biên chế; xác định vị trí việc làm, tiêu chuẩn chức danh, cơ cấu ngạch công chức, viên chức gắn với nhiệm vụ bảo vệ an ninh mạng tại các cơ quan, đơn vị.

- Phối hợp rà soát, đề xuất kế hoạch tuyển dụng, sử dụng, đào tạo, bồi dưỡng và phát triển đội ngũ cán bộ, công chức, viên chức làm công tác an ninh mạng; bảo đảm đủ số lượng, nâng cao chất lượng, đáp ứng yêu cầu nhiệm vụ trong tình hình mới.

6. Các sở, ban, ngành, Ủy ban nhân dân cấp xã

- Căn cứ chức năng, nhiệm vụ được giao và nội dung của Kế hoạch, tổ chức triển khai cụ thể tại địa phương. Hằng năm, **trước ngày 15/11** thực hiện chế độ thông tin, báo cáo định kỳ (hoặc đột xuất nếu có yêu cầu) về tình hình, kết quả triển khai gửi Công an tỉnh để tổng hợp, tham mưu theo quy định.

- Tổ chức triển khai các biện pháp bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin thuộc phạm vi quản lý; từng bước xây dựng, kiện toàn lực lượng tham gia bảo vệ an ninh mạng tại cơ sở, bảo đảm phù hợp với điều kiện thực tế và yêu cầu nhiệm vụ.

- Chủ động phối hợp với các cơ quan chức năng trong công tác phòng ngừa, phát hiện, xử lý và khắc phục sự cố an ninh mạng xảy ra tại địa phương; tham gia đầy đủ các hoạt động của đội ứng cứu sự cố an ninh mạng của tỉnh, bảo đảm kịp thời, hiệu quả, hạn chế thấp nhất thiệt hại có thể xảy ra.

- Tổ chức triển khai, duy trì thực hiện các phương án bảo đảm an toàn thông tin theo cấp độ đã được phê duyệt, bảo đảm 100% hệ thống thông tin thuộc phạm vi quản lý tuân thủ quy định về bảo đảm an toàn thông tin; kịp thời khắc phục các tồn tại, hạn chế, nâng cao năng lực phòng ngừa, phát hiện và xử lý sự cố an ninh mạng tại đơn vị.

7. Doanh nghiệp, tổ chức có liên quan

- Phối hợp với các cơ quan nhà nước trên địa bàn tỉnh trong việc triển khai các giải pháp bảo đảm an ninh mạng, an toàn thông tin; tham gia chia sẻ thông tin, cảnh báo nguy cơ, hỗ trợ xử lý sự cố an ninh mạng theo quy định, góp phần bảo đảm an toàn, ổn định hoạt động trên không gian mạng.

- Tập trung nghiên cứu, đầu tư, phát triển và sử dụng các sản phẩm, giải pháp an ninh mạng "Make in Vietnam"; nâng cao năng lực tự chủ công nghệ, bảo đảm phù hợp với tiêu chuẩn, quy chuẩn kỹ thuật và yêu cầu bảo đảm an ninh mạng hiện hành.

- Triển khai các biện pháp kỹ thuật, nghiệp vụ nhằm bảo đảm an toàn hệ thống thông tin, hạ tầng viễn thông, dịch vụ số do doanh nghiệp quản lý, vận hành. Thực hiện nghiêm các quy định của pháp luật về an ninh mạng.

Giao Công an tỉnh chủ trì, phối hợp với các sở, ngành, địa phương theo dõi, đôn đốc việc triển khai thực hiện Kế hoạch, kịp thời báo cáo và kiến nghị Ủy ban nhân dân tỉnh các biện pháp cần thiết để bảo đảm thực hiện đồng bộ và có hiệu quả; đồng thời tổng hợp báo cáo theo quy định. Quá trình triển khai, thực hiện, nếu có khó khăn, vướng mắc, các đơn vị, địa phương có văn bản gửi Công an tỉnh để tổng hợp và hướng dẫn giải quyết theo thẩm quyền hoặc trình cấp có thẩm quyền xem xét, quyết định./.

Nơi nhận:
- Bộ Công an (để báo cáo);
- Chủ tịch, các PCT UBND tỉnh;
- Các sở, ban, ngành thuộc tỉnh;
- UBND các xã, phường;
- Các DN viễn thông;
- CVP, PVP VX;
- Trung tâm PVHCC;
- Lưu: VT, V9.

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

ỦY BAN NHÂN DÂN TỈNH GIA LAI

Lâm Hải Giang

PHỤ LỤC

Danh mục các nhiệm vụ, giải pháp triển khai thực hiện Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia" trên địa bàn tỉnh Gia Lai

(Kèm theo Kế hoạch số /KH-UBND ngày / /2026 của UBND tỉnh Gia Lai)

STT	Nhiệm vụ	Cơ quan chủ trì	Cơ quan phối hợp	Thời gian thực hiện	Ghi chú
1	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, ngành, địa phương liên quan	Thường xuyên	
2	Tham mưu triển khai TCVN 11423:2025 trên cơ sở hợp nhất TCVN 11423:2025 và TCVN 11930:2017 cho các cấp độ hệ thống thông tin vận hành trên địa bàn tỉnh.	Công an tỉnh	Các sở, ngành, địa phương liên quan	Quý II/2026	Sau khi Bộ Công an ban hành tiêu chuẩn
3	Ban hành khung quản lý rủi ro an ninh mạng tỉnh, hướng dẫn các đơn vị trong quản lý rủi ro an ninh mạng.	Công an tỉnh	Các sở, ngành, địa phương liên quan	Quý IV/2026	Sau khi Bộ Công an ban hành Khung quản trị rủi ro an ninh mạng
4	Rà soát, đề xuất chính sách ưu đãi hỗ trợ doanh nghiệp đổi mới sáng tạo, làm chủ công nghệ, phát triển các sản phẩm, dịch vụ an ninh mạng trong nước.	Công an tỉnh, Sở Tài chính	Sở Khoa học và Công nghệ, các sở, ngành, địa phương liên quan	Thường xuyên	

5	Kiện toàn Tiểu ban An ninh mạng tỉnh.	Công an tỉnh	Văn phòng Tỉnh ủy, Văn phòng UBND tỉnh	Quý II/2026	
6	Rà soát, xây dựng tổ chức lực lượng bảo vệ an ninh mạng tại tỉnh.	Công an tỉnh	Các sở, ban, ngành, địa phương liên quan	2026 - 2027	Sau khi có hướng dẫn của Bộ Công an
7	Xây dựng, phát triển mạng lưới chuyên gia an ninh mạng trong và ngoài tỉnh tham gia hỗ trợ công tác bảo đảm an ninh mạng; kiện toàn, nâng cao năng lực Đội Ứng cứu sự cố an toàn thông tin mạng của tỉnh.	Công an tỉnh	Các cơ quan, đơn vị liên quan	Thường xuyên	
8	100% các hệ thống thông tin sử dụng vốn ngân sách nhà nước được triển khai đầy đủ các phương án bảo đảm an ninh mạng theo cấp độ.	Công an tỉnh	Các sở, ngành, địa phương liên quan	Quý III/2026	
9	Tổ chức đào tạo, bồi dưỡng, tập huấn nhằm nâng cao trình độ chuyên môn, kỹ năng nghiệp vụ và năng lực ứng phó, xử lý sự cố an ninh mạng, bảo đảm sẵn sàng đáp ứng yêu cầu trong mọi tình huống.	Công an tỉnh	Các sở, ngành, địa phương liên quan	Hằng năm	
10	Tổ chức ít nhất 01 đợt diễn tập chuyên đề an ninh mạng hoặc ứng cứu sự cố an toàn thông tin mạng cho cán bộ, công chức trên địa bàn tỉnh	Công an tỉnh	Các sở, ngành, địa phương liên quan	Hằng năm	
11	Phổ biến, nâng cao kiến thức an ninh mạng cho người dân qua các nền tảng học tập số, “Bình dân học vụ	Công an tỉnh	Sở Khoa học và Công nghệ;	Thường xuyên	

	số", các khóa học đại chúng mở (MOOC) và các chiến dịch truyền thông đại chúng.		các cơ quan, đơn vị liên quan		
12	Triển khai áp dụng 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 trên địa bàn.	Công an tỉnh	Các sở, ngành, địa phương liên quan	2026-2027	Sau khi Bộ Công an ban hành, hướng dẫn
13	Xây dựng, kết nối Trung tâm An ninh mạng tỉnh vào Trung tâm An ninh mạng quốc gia, chia sẻ, nâng cao năng lực giám sát.	Công an tỉnh		2026-2028	
14	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.	Công an tỉnh		Thường xuyên	Báo cáo kết quả thực hiện
15	Thúc đẩy phát triển các trung tâm kiểm định an ninh mạng theo hướng xã hội hóa, đủ năng lực thực hiện thử nghiệm, đánh giá sự phù hợp tiêu chuẩn, quy chuẩn đối với sản phẩm an ninh mạng.	Công an tỉnh	Các cơ quan, doanh nghiệp và hội, hiệp hội trong lĩnh vực an ninh mạng, CNTT.	2026-2027	Sau khi có hướng dẫn của Bộ Khoa học và Công nghệ, Bộ Công an