

Số: /KH-UBND

Vinh Long, ngày tháng năm 2026

KẾ HOẠCH

Triển khai thực hiện 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” trên địa bàn tỉnh Vĩnh Long

Thực hiện 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” (viết tắt là Đề án), Ủy ban nhân dân (UBND) tỉnh ban hành Kế hoạch triển khai thực hiện với những nội dung cụ thể, như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

a) Quán triệt, tổ chức triển khai thực hiện nghiêm túc, đầy đủ, hiệu quả các nội dung, nhiệm vụ, giải pháp của Đề án trên địa bàn tỉnh. Đề án xác định an ninh mạng là bộ phận của an ninh quốc gia, lực lượng bảo vệ an ninh mạng giữ vai trò nòng cốt trong phòng ngừa, phát hiện, đấu tranh, xử lý hành vi vi phạm pháp luật trên không gian mạng.

b) Nâng cao năng lực tổng thể của lực lượng bảo vệ an ninh mạng trên địa bàn tỉnh; tăng cường năng lực 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.

c) Cụ thể hóa các nhiệm vụ của Đề án phù hợp với chức năng, nhiệm vụ của các sở, ban, ngành tỉnh, UBND xã, phường và các cơ quan, đơn vị có liên quan.

2. Yêu cầu

a) Việc tổ chức thực hiện phải bám sát quan điểm, mục tiêu, nhiệm vụ của Đề án, việc triển khai thực hiện phải đồng bộ, thống nhất, thiết thực, hiệu quả; bám sát nội dung Đề án.

b) Xác định rõ trách nhiệm của cơ quan chủ trì, cơ quan phối hợp, thời gian thực hiện; bảo đảm sự phối hợp chặt chẽ giữa các cơ quan, đơn vị, địa phương trong tổ chức thực hiện.

c) Ưu tiên bố trí nguồn lực phù hợp để triển khai các nhiệm vụ bảo đảm an ninh mạng trong hoạt động nội bộ của cơ quan, tổ chức và lĩnh vực quản lý; đồng thời tổ chức diễn tập, đào tạo, tập huấn, trang bị hệ thống, công cụ chuyên dụng theo đúng định hướng Đề án giao cho các bộ, ngành, địa phương.

II. MỤC TIÊU

1. Mục tiêu tổng quát

Xây dựng lực lượng bảo vệ an ninh mạng tỉnh hiện đại, 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 đến năm 2030

a) Phân đầu 100% lực lượng chuyên trách bảo vệ an ninh mạng cấp tỉnh được đào tạo, cập nhật kiến thức về an ninh mạng ít nhất 01 lần/năm; 100% hệ thống thông tin cấp độ 3 trở lên và 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; 100% sở, ban, ngành, UBND các xã, phường phân công có đầu mối phụ trách về an ninh mạng tại đơn vị.

b) Tối thiểu 70% các cơ quan, đơn vị ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng “Make in Vietnam”.

c) Hằng năm, tổ chức ít nhất 01 cuộc diễn tập bảo vệ an ninh mạng quy mô cấp tỉnh. Có 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 an ninh mạng.

3. Tầm nhìn đến năm 2045

Lực lượng chuyên trách bảo vệ an ninh mạng cấp tỉnh có năng lực mạnh trong phòng thủ, tấn công trấn áp tội phạm mạng và các thế lực thù địch, bảo vệ mọi hoạt động của Nhà nước, doanh nghiệp trên không gian mạng.

III. NỘI DUNG VÀ PHÂN CÔNG THỰC HIỆN

1. Tổ chức triển khai, quán triệt đầy đủ nội dung của Đề án

- Đơn vị thực hiện: Các cơ quan, đơn vị, địa phương trên địa bàn tỉnh.
- Thời gian thực hiện: Thường xuyên.

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

a) Rà soát, cập nhật các văn bản quy phạm pháp luật có nội dung liên quan đến bảo đảm an ninh mạng; kịp thời tham mưu sửa đổi, bổ sung hoặc kiến nghị cấp có thẩm quyền sửa đổi, bổ sung các nội dung chưa phù hợp với yêu cầu công tác bảo vệ an ninh mạng.

- Cơ quan chủ trì: Công an tỉnh.
- Cơ quan phối hợp: Sở Tư pháp; Sở Khoa học và Công nghệ; các sở, ban, ngành tỉnh; UBND xã, phường; các cơ quan, đơn vị liên quan.
- Thời gian thực hiện: Thường xuyên.

b) Tổ chức quán triệt, triển khai các quy định, tiêu chuẩn, quy chuẩn kỹ thuật, hướng dẫn chuyên ngành về an ninh mạng, an toàn thông tin, quản lý rủi ro an ninh mạng và bảo vệ hệ thống thông tin theo chỉ đạo của cơ quan cấp trên.

- Cơ quan chủ trì: Sở Khoa học và Công nghệ; Công an tỉnh theo chức năng, nhiệm vụ.

- Cơ quan phối hợp: Các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên.

3. Tổ chức lực lượng an ninh mạng

a) Rà soát, kiện toàn Tiểu ban An ninh mạng tỉnh, lực lượng chuyên trách bảo vệ an ninh mạng; đầu mối, lực lượng làm công tác bảo vệ an ninh mạng tại các cơ quan, đơn vị, địa phương; bố trí cán bộ phù hợp với vị trí việc làm, bảo đảm đáp ứng yêu cầu quản lý, vận hành, bảo vệ hệ thống thông tin quan trọng và an ninh quốc gia. 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 trên địa bàn tỉnh.

- Cơ quan chủ trì: Công an tỉnh.

- Cơ quan phối hợp: Sở Nội vụ; các sở, ban, ngành tỉnh; UBND xã, phường; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên.

b) Xây dựng, củng cố cơ chế phối hợp, trao đổi thông tin, hỗ trợ xử lý các vấn đề phát sinh giữa lực lượng bảo vệ an ninh mạng với các cơ quan, đơn vị quản trị, vận hành hệ thống thông tin, doanh nghiệp viễn thông, công nghệ thông tin và các cơ quan, đơn vị khác có liên quan trên địa bàn tỉnh. Hình thành đội ngũ chuyên gia về an ninh mạng có năng lực về giám sát, vận hành Hệ thống giám sát an ninh mạng tỉnh; điều tra số; phân tích mã độc; đánh giá lỗ hổng, kiểm thử thông tin; ứng cứu sự cố an ninh mạng.

- Cơ quan chủ trì: Công an tỉnh.

- Cơ quan phối hợp: Sở Khoa học và Công nghệ; các doanh nghiệp viễn thông, công nghệ thông tin; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên.

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

a) Tổ chức đào tạo, bồi dưỡng, tập huấn trực tiếp hoặc trực tuyến về bảo đảm an ninh mạng; ứng cứu sự cố, kỹ năng nhận diện và xử lý nguy cơ mất an ninh mạng cho cán bộ lãnh đạo, quản lý, cán bộ chuyên trách, cán bộ kỹ thuật và người dùng trong cơ quan nhà nước.

- Cơ quan chủ trì: Công an tỉnh.

- Cơ quan phối hợp: Sở Nội vụ; Sở Giáo dục và Đào tạo; Sở Khoa học và Công nghệ; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Hằng năm.

b) Rà soát đội ngũ cán bộ trực tiếp quản trị, vận hành hệ thống thông tin; xây dựng kế hoạch bồi dưỡng, cập nhật kiến thức, kỹ năng chuyên sâu, khuyến khích đào tạo gắn với tiêu chuẩn, chứng chỉ chuyên môn phù hợp, bảo đảm 100% lực lượng chuyên trách bảo vệ an ninh mạng đáp ứng các yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng, được cập nhật kiến thức an ninh mạng ít nhất 01 lần/năm.

- Cơ quan chủ trì: Các sở, ban, ngành tỉnh; UBND xã, phường theo chức năng, nhiệm vụ.

- Cơ quan phối hợp: Công an tỉnh; Sở Nội vụ; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên.

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

a) Tăng cường giám sát hoạt động của các hệ thống thông tin, tổ chức rà soát, đánh giá thực trạng bảo đảm an ninh mạng đối với các hệ thống thông tin, cơ sở dữ liệu, nền tảng số thuộc phạm vi quản lý; kịp thời phát hiện sơ hở, thiếu sót, nguy cơ mất an ninh mạng để có biện pháp xử lý, khắc phục.

- Cơ quan chủ trì: Các sở, ban, ngành tỉnh; UBND xã, phường theo chức năng, nhiệm vụ.

- Cơ quan phối hợp: Công an tỉnh; Sở Khoa học và Công nghệ; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên.

b) Tăng cường cơ chế cung cấp, tiếp nhận, chia sẻ, cảnh báo thông tin về nguy cơ, sự cố, vụ việc an ninh mạng giữa các cơ quan, đơn vị, địa phương; phối hợp xử lý, ứng cứu, khắc phục sự cố kịp thời, hiệu quả.

- Cơ quan chủ trì: Công an tỉnh.

- Cơ quan phối hợp: Sở Khoa học và Công nghệ; Văn phòng UBND tỉnh; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên.

c) Hằng năm, tổ chức ít nhất 01 cuộc diễn tập bảo vệ an ninh mạng, ứng cứu sự cố mạng trong phạm vi quản lý; tổ chức đào tạo, tập huấn, diễn tập phù hợp theo hướng dẫn của Bộ Công an.

- Cơ quan chủ trì: Công an tỉnh.

- Cơ quan phối hợp: Các sở, ban, ngành tỉnh; UBND xã, phường; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Hằng năm.

d) Trang bị hệ thống, thiết bị chuyên dụng cho lực lượng bảo vệ an ninh mạng, gồm hệ thống, công cụ rà quét, phát hiện lỗ hổng bảo mật; hệ thống, công cụ phục vụ điều tra số; ứng cứu sự cố, giám sát, phát hiện, cảnh báo nguy cơ mất an ninh mạng.

- Cơ quan chủ trì: Công an tỉnh.
- Cơ quan phối hợp: Sở Tài chính; Sở Khoa học và Công nghệ; các cơ quan, đơn vị liên quan.
- Thời gian thực hiện: Theo kế hoạch hằng năm và giai đoạn 2026 - 2030.

6. Nghiên cứu phát triển, nâng cao năng lực tự chủ công nghệ, đặc biệt để từng bước làm chủ các công nghệ lõi trong lĩnh vực an ninh mạng

a) Tăng cường nghiên cứu, ứng dụng khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số phục vụ công tác bảo vệ an ninh mạng; ưu tiên nghiên cứu, thử nghiệm, ứng dụng các sản phẩm, giải pháp, dịch vụ an ninh mạng do doanh nghiệp Việt Nam phát triển, làm chủ công nghệ, phù hợp điều kiện thực tế của tỉnh. Trong đó, ít nhất 70% các sở, ngành tỉnh, địa phương và các hệ thống thông tin quan trọng quốc gia (nếu có) 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.

- Cơ quan chủ trì: Sở Khoa học và Công nghệ; Công an tỉnh theo chức năng, nhiệm vụ.
- Cơ quan phối hợp: Các sở, ban, ngành tỉnh; các doanh nghiệp liên quan; các cơ quan, đơn vị liên quan.
- Thời gian thực hiện: Thường xuyên.

b) Tổ chức rà soát, đánh giá an ninh mạng đối với hệ thống thông tin cấp độ 3 trở lên; kiểm tra việc triển khai phương án bảo đảm an ninh mạng tại các cơ quan, đơn vị.

- Cơ quan chủ trì: Công an tỉnh; Sở Khoa học và Công nghệ theo chức năng, nhiệm vụ.
- Cơ quan phối hợp: Các sở, ban, ngành tỉnh; các doanh nghiệp liên quan; các cơ quan, đơn vị liên quan.
- Thời gian thực hiện: Hằng năm.

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

a) Chủ động phối hợp triển khai các hoạt động phối hợp, trao đổi kinh nghiệm, tiếp cận mô hình, sáng kiến, tiêu chuẩn, thực tiễn tốt về an ninh mạng theo hướng dẫn, điều phối của các bộ, ngành Trung ương; góp phần nâng cao năng lực bảo vệ an ninh mạng trên địa bàn tỉnh.

- Cơ quan chủ trì: Công an tỉnh.

- Cơ quan phối hợp: Văn phòng UBND tỉnh; Sở Khoa học và Công nghệ; các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên.

b) Tạo điều kiện cho cán bộ, công chức, viên chức thuộc phạm vi quản lý tham gia các hoạt động tập huấn, hội thảo, diễn đàn, chương trình hợp tác quốc tế về an ninh mạng khi có yêu cầu, bảo đảm đúng quy định của pháp luật và phù hợp với điều kiện thực tế của địa phương.

- Cơ quan chủ trì: Sở Nội vụ; Văn phòng UBND tỉnh; Công an tỉnh theo chức năng, nhiệm vụ.

- Cơ quan phối hợp: Các cơ quan, đơn vị liên quan.

- Thời gian thực hiện: Thường xuyên.

IV. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch này do ngân sách nhà nước hằng năm bảo đảm theo phân cấp hiện hành và các nguồn kinh phí hợp pháp khác theo quy định của pháp luật.

V. TỔ CHỨC THỰC HIỆN

1. Các sở, ban, ngành tỉnh; UBND xã, phường

a) Thủ trưởng các sở, ban, ngành tỉnh và UBND các xã, phường chức năng, nhiệm vụ được phân công và phạm vi quản lý chủ động tổ chức triển khai thực hiện phù hợp với tình hình thực tế, bảo đảm hiệu quả.

Định kỳ hằng năm hoặc khi có yêu cầu; theo chức năng, nhiệm vụ được giao, các sở, ban, ngành tỉnh và UBND các xã, phường báo cáo tình hình, kết quả thực hiện Kế hoạch về Công an tỉnh (qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) để tổng hợp, tham mưu UBND tỉnh báo cáo Chính phủ, Bộ Công an theo quy định.

b) Tổ chức quán triệt, phổ biến nội dung Kế hoạch này và các quy định của pháp luật có liên quan đến toàn thể cán bộ, công chức, viên chức, người lao động thuộc phạm vi quản lý; nâng cao nhận thức, trách nhiệm của người đứng đầu trong công tác bảo vệ an ninh mạng.

c) Chủ động rà soát, đánh giá hiện trạng bảo đảm an ninh mạng đối với hệ thống thông tin, cơ sở dữ liệu, nền tảng số thuộc phạm vi quản lý; kịp thời phát hiện, khắc phục sơ hở, thiếu sót, nguy cơ mất an ninh mạng; phối hợp chặt chẽ với Công an tỉnh trong xử lý các tình huống, vụ việc phát sinh.

d) Bố trí nguồn lực phù hợp để triển khai các nhiệm vụ bảo đảm an ninh mạng trong hoạt động nội bộ của cơ quan, đơn vị, địa phương và lĩnh vực quản lý.

e) Cử cán bộ tham gia đầy đủ các lớp đào tạo, tập huấn, bồi dưỡng, diễn tập do cơ quan có thẩm quyền tổ chức; đồng thời chủ động tổ chức hoặc phối hợp tổ

chức các hoạt động tuyên truyền, hướng dẫn, bồi dưỡng nội bộ phù hợp với điều kiện thực tế.

g) Phối hợp bảo đảm an ninh mạng ngay từ giai đoạn thiết kế, đầu tư, triển khai các nền tảng số, cơ sở dữ liệu, hệ thống thông tin phục vụ chuyển đổi số của tỉnh.

2. Công an tỉnh

a) Là cơ quan đầu mối, chủ trì tham mưu UBND tỉnh tổ chức triển khai thực hiện Kế hoạch này trên phạm vi toàn tỉnh; chủ động hướng dẫn, đôn đốc, kiểm tra các sở, ban, ngành tỉnh, UBND xã, phường và các cơ quan, đơn vị có liên quan trong quá trình tổ chức thực hiện.

b) Tham mưu rà soát, kiện toàn đầu mối, lực lượng bảo vệ an ninh mạng; hướng dẫn các cơ quan, đơn vị, địa phương rà soát, bố trí cán bộ trực tiếp tham mưu, quản trị, vận hành, bảo vệ hệ thống thông tin thuộc phạm vi quản lý theo yêu cầu nhiệm vụ.

c) Tổ chức hoặc phối hợp tổ chức các hoạt động đào tạo, tập huấn, bồi dưỡng, cập nhật kiến thức, kỹ năng về bảo vệ an ninh mạng; ứng cứu sự cố, giám sát, phát hiện, xử lý nguy cơ mất an ninh mạng cho cán bộ, công chức, viên chức, người lao động và lực lượng trực tiếp thực hiện nhiệm vụ trong các cơ quan nhà nước trên địa bàn tỉnh; nội dung đào tạo, gồm: Nghiệp vụ quản lý và kỹ năng bảo đảm an ninh mạng cho đội ngũ lãnh đạo, quản lý; nghiệp vụ an ninh mạng cho lực lượng chuyên trách bảo vệ an ninh mạng; kiến thức, kỹ năng bảo đảm an ninh mạng của người dùng cho cán bộ công chức, viên chức, người lao động và các đối tượng có liên quan theo quy định của pháp luật.

d) Tham mưu tổ chức ít nhất 01 cuộc/năm diễn tập bảo vệ an ninh mạng, ứng cứu sự cố trong năm phù hợp với điều kiện thực tế của địa phương; hướng dẫn các cơ quan, đơn vị, địa phương xây dựng phương án, kịch bản diễn tập, rút kinh nghiệm sau diễn tập để nâng cao năng lực thực hành, hiệp đồng, phối hợp xử lý tình huống.

e) Tham mưu đầu tư, trang bị, nâng cấp hệ thống, thiết bị chuyên dụng phục vụ công tác bảo vệ an ninh mạng, gồm công cụ rà quét, phát hiện lỗ hổng bảo mật; công cụ điều tra số; công cụ ứng cứu sự cố; hệ thống giám sát, phát hiện, cảnh báo nguy cơ mất an ninh mạng; bảo đảm phù hợp quy định, tiêu chuẩn, định mức và khả năng cân đối ngân sách.

g) Tham mưu xây dựng, củng cố cơ chế tiếp nhận, tổng hợp, phân tích, chia sẻ, cảnh báo thông tin về nguy cơ, sự cố, vụ việc an ninh mạng giữa các cơ quan, đơn vị, địa phương; kịp thời phối hợp tham mưu xử lý các tình huống phát sinh, không để bị động, bất ngờ.

h) Định kỳ hằng năm hoặc đột xuất, chủ trì kiểm tra kết quả thực hiện Kế hoạch tại các cơ quan, đơn vị, địa phương; tham mưu sơ kết, tổng kết và tổng hợp tình hình, kết quả thực hiện, tham mưu UBND tỉnh báo cáo Bộ Công an và cơ quan có thẩm quyền theo quy định; đề xuất biểu dương, khen thưởng các tập thể,

cá nhân có thành tích; đồng thời kiến nghị chấn chỉnh, xem xét trách nhiệm đối với cơ quan, đơn vị, cá nhân thực hiện chưa nghiêm túc, không bảo đảm tiến độ, chất lượng theo yêu cầu.

3. Sở Khoa học và Công nghệ

a) Tham mưu triển khai các nhiệm vụ về ứng dụng khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số phục vụ công tác bảo vệ an ninh mạng trên địa bàn tỉnh.

b) Chủ trì hoặc phối hợp rà soát, hướng dẫn áp dụng tiêu chuẩn, quy chuẩn kỹ thuật, yêu cầu kỹ thuật, giải pháp công nghệ phù hợp trong công tác bảo đảm an ninh mạng đối với các hệ thống thông tin thuộc phạm vi quản lý của tỉnh.

c) Phối hợp nghiên cứu, đề xuất, tham mưu thúc đẩy sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng do doanh nghiệp Việt Nam nghiên cứu, làm chủ công nghệ, phù hợp với điều kiện thực tế của địa phương.

d) Phối hợp với Công an tỉnh và các cơ quan liên quan rà soát, đánh giá hiện trạng, đề xuất phương án nâng cấp hạ tầng kỹ thuật, hệ thống thông tin, nền tảng số, cơ sở dữ liệu dùng chung gắn với yêu cầu bảo đảm an ninh mạng.

4. Bộ Chỉ huy Quân sự tỉnh

a) Phối hợp với Công an tỉnh trong trao đổi thông tin, nắm tình hình, bảo vệ an ninh mạng, đấu tranh, ngăn chặn các hoạt động xâm phạm an ninh mạng liên quan đến quốc phòng, an ninh trên địa bàn tỉnh theo chức năng, nhiệm vụ được giao.

b) Chỉ đạo tăng cường công tác bảo vệ an ninh mạng, an toàn thông tin đối với hệ thống thông tin, thiết bị, dữ liệu thuộc phạm vi quản lý; chủ động rà soát, khắc phục sơ hở, thiếu sót, nguy cơ mất an ninh mạng.

c) Phối hợp tham gia diễn tập, tập huấn, chia sẻ kinh nghiệm, phương án phối hợp xử lý tình huống liên quan đến an ninh mạng.

5. Sở Giáo dục và Đào tạo

a) Phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ tổ chức tuyên truyền, phổ biến kiến thức, kỹ năng cơ bản về an ninh mạng, sử dụng không gian mạng an toàn cho đội ngũ cán bộ quản lý giáo dục, giáo viên, học sinh, học viên phù hợp với chức năng, nhiệm vụ được giao.

b) Chỉ đạo các cơ sở giáo dục thuộc phạm vi quản lý tăng cường bảo đảm an ninh mạng đối với hệ thống thông tin, nền tảng dạy học, quản lý giáo dục; chủ động rà soát, phát hiện nguy cơ, lỗ hổng, sơ hở để có biện pháp khắc phục.

c) Phối hợp trong công tác tập huấn, bồi dưỡng, nâng cao nhận thức và kỹ năng ứng phó với các nguy cơ mất an ninh mạng trong môi trường giáo dục số.

6. Sở Tài chính

a) Căn cứ nhiệm vụ được giao tại Kế hoạch này, phối hợp với Công an tỉnh và các cơ quan, đơn vị liên quan tham mưu UBND tỉnh bố trí kinh phí thực hiện theo phân cấp ngân sách và quy định của pháp luật.

b) Hướng dẫn các cơ quan, đơn vị, địa phương lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện Kế hoạch đúng quy định; ưu tiên tham mưu bố trí kinh phí cho các nhiệm vụ trọng tâm, cấp bách, trực tiếp phục vụ nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng.

c) Tham mưu huy động các nguồn lực hợp pháp khác để triển khai các nhiệm vụ của Kế hoạch theo quy định.

7. Sở Nội vụ

a) Phối hợp với Công an tỉnh rà soát, tham mưu kiện toàn tổ chức, đầu mối, vị trí việc làm, bố trí nhân lực làm công tác bảo vệ an ninh mạng tại các cơ quan, đơn vị, địa phương theo quy định.

b) Phối hợp tham mưu lồng ghép nội dung nâng cao năng lực đội ngũ cán bộ làm công tác bảo vệ an ninh mạng vào kế hoạch đào tạo, bồi dưỡng cán bộ, công chức, viên chức hằng năm của tỉnh.

c) Phối hợp nghiên cứu, đề xuất các giải pháp phù hợp nhằm nâng cao chất lượng đội ngũ cán bộ thực hiện nhiệm vụ bảo vệ an ninh mạng trong cơ quan nhà nước.

8. Văn phòng UBND tỉnh

a) Phối hợp với Công an tỉnh và các cơ quan liên quan tham mưu thực hiện các nội dung hợp tác quốc tế về an ninh mạng theo quy định của pháp luật, phù hợp với phân cấp, thẩm quyền và yêu cầu thực tế của địa phương.

b) Phối hợp tham mưu tạo điều kiện cho cán bộ, công chức, viên chức của tỉnh tham gia các hoạt động hội thảo, đào tạo, trao đổi kinh nghiệm quốc tế về an ninh mạng khi có yêu cầu và bảo đảm điều kiện theo quy định.

9. Các cơ quan Trung ương đóng trên địa bàn tỉnh; các doanh nghiệp viễn thông, công nghệ số; tổ chức, doanh nghiệp có liên quan

a) Phối hợp với Công an tỉnh, Sở Khoa học và Công nghệ và các cơ quan liên quan trong chia sẻ thông tin, cảnh báo nguy cơ, hỗ trợ kỹ thuật, rà quét, phát hiện, ngăn chặn, xử lý sự cố, vụ việc phức tạp về an ninh mạng theo quy định của pháp luật.

b) Chủ động rà soát, nâng cao năng lực bảo đảm an ninh mạng đối với hệ thống, hạ tầng, nền tảng, dịch vụ do đơn vị quản lý, vận hành; phối hợp thực hiện các yêu cầu bảo đảm an ninh mạng của cơ quan có thẩm quyền.

c) Tham gia, hỗ trợ các hoạt động đào tạo, tập huấn, diễn tập, nghiên cứu, thử nghiệm, chuyển giao công nghệ, phát triển và ứng dụng các sản phẩm, giải pháp an ninh mạng trong nước khi được đề nghị và phù hợp với chức năng, khả năng của doanh nghiệp.

10. Kể từ ngày Kế hoạch này có hiệu lực, các Kế hoạch sau hết hiệu lực thi hành:

- Kế hoạch số 94/KH-UBND ngày 17/3/2026 của Chủ tịch UBND tỉnh Vĩnh Long về đào tạo nguồn nhân lực an ninh mạng đến năm 2030;

- Kế hoạch số 258/KH-UBND ngày 01/12/2022 của Chủ tịch UBND tỉnh Bến Tre về đào tạo nguồn nhân lực an ninh mạng đến năm 2025, tầm nhìn đến năm 2030;

- Kế hoạch số 233/KH-UBND ngày 31/10/2022 của Chủ tịch UBND tỉnh Vĩnh Long về đào tạo nguồn nhân lực an ninh mạng đến năm 2025, tầm nhìn đến năm 2030 trên địa bàn tỉnh;

Trong quá trình tổ chức thực hiện, có phát sinh khó khăn, vướng mắc, các cơ quan, đơn vị, địa phương kịp thời báo cáo về Công an tỉnh để được hướng dẫn thực hiện hoặc tổng hợp báo cáo cấp có thẩm quyền xem xét, quyết định./.

Nơi nhận:

- Văn phòng Chính phủ;
- Bộ Công an;
- Thường trực Tỉnh ủy, HĐND tỉnh;
- Chủ tịch, các PCT UBND tỉnh;
- Các sở, ban, ngành tỉnh;
- Cơ quan TW đóng trên địa bàn tỉnh;
- Các doanh nghiệp viễn thông;
- Các trường Đại học, Cao đẳng trên địa bàn tỉnh;
- Báo và PTTH Vĩnh Long;
- UBND các xã, phường;
- Chánh, PCVP UBND tỉnh;
- Phòng: NC, KGVX, NgV, TH;
- Lưu: VT, NC (PT).

CHỦ TỊCH

Trần Trí Quang