

Số: /KH-UBND

An Giang, 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 An Giang

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”; Ủy ban nhân dân tỉnh ban hành Kế hoạch triển khai thực hiện; cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục tiêu

1.1. Mục tiêu tổng quát

- Triển khai thực hiện nghiêm túc, đồng bộ, 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”; xây dựng lực lượng bảo vệ an ninh mạng trên địa bàn tỉnh An Giang theo hướng tinh nhuệ, hiện đại, đủ năng lực chủ động phòng ngừa, phát hiện, đấu tranh, xử lý hiệu quả các nguy cơ, thách thức trên không gian mạng; bảo vệ vững chắc an ninh quốc gia, trật tự an toàn xã hội, phục vụ hiệu quả nhiệm vụ phát triển kinh tế - xã hội, chuyển đổi số và hội nhập quốc tế trong tình hình mới.

- Xác định đây là nhiệm vụ chính trị trọng tâm, thường xuyên, lâu dài của cả hệ thống chính trị; gắn công tác bảo vệ an ninh mạng với nhiệm vụ phát triển kinh tế - xã hội, xây dựng chính quyền số, kinh tế số, xã hội số và bảo vệ chủ quyền quốc gia trên không gian mạng.

1.2. Mục tiêu cụ thể đến năm 2030

- Phân đầu nâng cao toàn diện năng lực hoạt động của lực lượng bảo vệ an ninh mạng trên địa bàn tỉnh; xây dựng lực lượng chuyên trách, bán chuyên trách đủ khả năng xử lý các tình huống an ninh mạng phức tạp, không để bị động, bất ngờ trong mọi tình huống.

- 100% lực lượng chuyên trách bảo vệ an ninh mạng thuộc Công an tỉnh; cán bộ phụ trách công nghệ thông tin, quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5 tại các cơ quan Nhà nước trên địa bàn được đào tạo, bồi dưỡng, cập nhật kiến thức an ninh mạng tối thiểu 01 lần/năm; từng bước đáp ứng

yêu cầu chuẩn kiến thức, kỹ năng chuyên sâu về an ninh mạng theo quy định của cơ quan có thẩm quyền.

- Phần đầu 100% hệ thống thông tin sử dụng ngân sách nhà nước trên địa bàn tỉnh được triển khai đầy đủ phương án bảo đảm an ninh mạng theo cấp độ; các hệ thống thông tin trọng yếu được giám sát, kiểm tra, đánh giá an toàn thông tin định kỳ.

- Từng bước hình thành năng lực giám sát, cảnh báo sớm nguy cơ mất an ninh mạng trên địa bàn tỉnh; nâng cao khả năng ứng cứu, xử lý sự cố an toàn thông tin mạng đối với các hệ thống thông tin quan trọng.

- Phần đầu trên 90% cán bộ, công chức, viên chức và người sử dụng Internet trên địa bàn tỉnh được tuyên truyền, phổ biến kiến thức, kỹ năng cơ bản về an ninh mạng, nhận diện và phòng ngừa các nguy cơ lừa đảo trực tuyến, xâm phạm dữ liệu cá nhân và tội phạm sử dụng công nghệ cao.

- Tăng cường sử dụng các sản phẩm, giải pháp công nghệ thông tin, an ninh mạng “Make in Vietnam” trong cơ quan Nhà nước; ưu tiên triển khai đối với các hệ thống thông tin quan trọng, hệ thống phục vụ chỉ đạo điều hành, cơ sở dữ liệu chuyên ngành và nền tảng số dùng chung của tỉnh.

- Tăng cường năng lực phòng ngừa, đấu tranh với các loại tội phạm sử dụng công nghệ cao; tập trung kéo giảm các vụ việc lừa đảo chiếm đoạt tài sản trên không gian mạng, mua bán dữ liệu cá nhân, tấn công mạng, phát tán mã độc và hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia.

- Từng bước xây dựng thể trận an ninh nhân dân trên không gian mạng; phát huy vai trò của Nhân dân, doanh nghiệp, tổ chức xã hội trong bảo vệ chủ quyền, lợi ích quốc gia trên không gian mạng theo đúng tinh thần Quyết định số 515/QĐ-TTg.

2. Yêu cầu

- Việc triển khai thực hiện Kế hoạch phải được tiến hành nghiêm túc, đồng bộ, thường xuyên, liên tục, có lộ trình cụ thể, phù hợp với tình hình thực tiễn của tỉnh An Giang và yêu cầu bảo vệ an ninh quốc gia trong giai đoạn mới. Xác định đây là kế hoạch lớn, có tính chiến lược, lâu dài, gắn với tiến trình chuyển đổi số quốc gia, xây dựng chính quyền số, kinh tế số, xã hội số và Chiến lược bảo vệ Tổ quốc trên không gian mạng.

- Các nhiệm vụ, giải pháp phải được triển khai đồng bộ giữa công tác xây dựng lực lượng, đào tạo nguồn nhân lực, đầu tư hạ tầng kỹ thuật, hiện đại hóa trang thiết bị, nâng cao năng lực giám sát, cảnh báo sớm nguy cơ mất an ninh mạng và nâng cao hiệu quả công tác phòng ngừa, đấu tranh với các hành vi vi phạm pháp luật trên không gian mạng; bảo đảm thiết thực, hiệu quả, tránh hình thức, chồng chéo.

- Công tác bảo vệ an ninh mạng phải được triển khai song hành với quá trình xây dựng chính quyền số, phát triển kinh tế số, xã hội số; bảo đảm nguyên tắc “an ninh mạng đi trước một bước”, không đánh đổi an ninh mạng để lấy tốc độ phát triển công nghệ và chuyển đổi số. Các nền tảng số, cơ sở dữ liệu, hệ thống thông tin mới phải được tích hợp giải pháp bảo đảm an ninh mạng ngay từ khâu thiết kế, xây dựng và vận hành.

- Các sở, ban, ngành, địa phương phải xác định công tác bảo vệ an ninh mạng là nhiệm vụ chính trị quan trọng, thường xuyên; chủ động xây dựng kế hoạch triển khai phù hợp với chức năng, nhiệm vụ được giao. Người đứng đầu cơ quan, đơn vị chịu trách nhiệm trực tiếp trước Ủy ban nhân dân tỉnh nếu để xảy ra tình trạng mất an ninh mạng, lộ lọt bí mật nhà nước, mất dữ liệu hoặc để các đối tượng lợi dụng không gian mạng hoạt động vi phạm pháp luật kéo dài mà không phát hiện, xử lý kịp thời.

II. NHIỆM VỤ, GIẢI PHÁP TRỌNG TÂM

1. Hoàn thiện thể chế, cơ chế, chính sách về bảo đảm an ninh mạng, tạo nền tảng pháp lý đồng bộ cho phát triển bền vững không gian số

- Tập trung rà soát, cập nhật, bổ sung và hoàn thiện hệ thống văn bản quy phạm pháp luật, quy chế, quy định, quy trình nghiệp vụ liên quan đến công tác bảo đảm an ninh mạng trên địa bàn tỉnh bảo đảm đồng bộ, thống nhất, phù hợp với tình hình thực tiễn và yêu cầu nhiệm vụ trong giai đoạn mới. Chủ động triển khai thực hiện hiệu quả Luật An ninh mạng, các văn bản hướng dẫn thi hành và các quy định liên quan đến bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân, an toàn thông tin mạng, phòng chống tội phạm sử dụng công nghệ cao.

- Chỉ đạo các sở, ban, ngành và địa phương tăng cường rà soát các quy chế quản lý, vận hành, khai thác và sử dụng hệ thống thông tin; bổ sung quy định phân công trách nhiệm cụ thể đối với người đứng đầu cơ quan, đơn vị trong công tác bảo đảm an ninh mạng. Đẩy mạnh xây dựng cơ chế phối hợp liên ngành trong công tác phát hiện, ngăn chặn, xử lý hoạt động tấn công mạng, lộ lọt dữ liệu, phát tán thông tin xấu độc, xuyên tạc, chống phá trên không gian mạng.

- Chủ động nghiên cứu, đề xuất cơ chế, chính sách đặc thù nhằm thu hút, đào tạo, bồi dưỡng, trọng dụng nguồn nhân lực chất lượng cao trong lĩnh vực an ninh mạng; khuyến khích các tổ chức, doanh nghiệp đầu tư phát triển sản phẩm, dịch vụ an ninh mạng “Make in Vietnam”, phục vụ yêu cầu bảo vệ hệ thống thông tin và chuyển đổi số của tỉnh.

- Từng bước triển khai mô hình quản trị rủi ro an ninh mạng theo hướng hiện đại, chuyển từ tư duy “ứng phó bị động” sang “chủ động phòng ngừa”, lấy phòng ngừa là chính; tăng cường đánh giá nguy cơ, dự báo sớm các mối đe dọa trên không gian mạng để kịp thời có phương án bảo vệ phù hợp.

2. Kiện toàn tổ chức bộ máy, nâng cao hiệu quả phối hợp và xây dựng lực lượng bảo vệ an ninh mạng chính quy, tinh nhuệ

- Tiếp tục kiện toàn Tiểu ban An ninh mạng tỉnh An Giang; nâng cao hiệu quả hoạt động của các tổ công tác, bộ phận chuyên trách về an ninh mạng tại các sở, ngành, địa phương. Xác định rõ trách nhiệm của từng cơ quan, đơn vị trong công tác bảo vệ chủ quyền, lợi ích quốc gia trên không gian mạng gắn với nhiệm vụ phát triển kinh tế - xã hội và bảo đảm quốc phòng, an ninh.

- Chỉ đạo các cơ quan, đơn vị rà soát, bố trí lực lượng phụ trách công nghệ thông tin, an toàn thông tin, an ninh mạng phù hợp với yêu cầu nhiệm vụ; từng bước xây dựng lực lượng chuyên trách có trình độ chuyên môn sâu, đủ năng lực giám sát, quản trị, vận hành và bảo vệ hệ thống thông tin trọng yếu của tỉnh.

- Tăng cường cơ chế phối hợp giữa Công an tỉnh An Giang với các sở, ngành, địa phương, doanh nghiệp viễn thông, doanh nghiệp công nghệ số trong công tác bảo đảm an ninh mạng, phòng chống tội phạm sử dụng công nghệ cao, xử lý tin giả, tin sai sự thật và bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng.

- Đẩy mạnh kết nối, chia sẻ thông tin với các cơ quan chức năng Trung ương; tham gia mạng lưới ứng cứu sự cố an ninh mạng quốc gia; chủ động phối hợp với các doanh nghiệp, chuyên gia, tổ chức nghiên cứu nhằm nâng cao khả năng phát hiện sớm, cảnh báo và ứng phó hiệu quả với các nguy cơ mất an ninh mạng.

3. Đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao đáp ứng yêu cầu nhiệm vụ trong tình hình mới

- Xác định công tác đào tạo, phát triển nguồn nhân lực là nhiệm vụ trọng tâm, mang tính chiến lược lâu dài trong bảo đảm an ninh mạng. Tổ chức khảo sát, đánh giá thực trạng năng lực đội ngũ cán bộ, công chức, viên chức và lực lượng chuyên trách để xây dựng kế hoạch đào tạo phù hợp với từng nhóm đối tượng.

- Hằng năm tổ chức các lớp đào tạo, tập huấn, bồi dưỡng kiến thức, kỹ năng về an ninh mạng cho đội ngũ lãnh đạo, quản lý nhằm nâng cao nhận thức, trách nhiệm trong công tác chỉ đạo, điều hành và xử lý tình huống an ninh mạng. Đồng thời, tăng cường đào tạo kỹ năng bảo đảm an toàn thông tin cho cán bộ, công chức, viên chức, người lao động trong quá trình sử dụng hệ thống thông tin, dịch vụ số và môi trường mạng.

- Tập trung huấn luyện chuyên sâu cho lực lượng trực tiếp quản trị, vận hành hệ thống thông tin cấp độ cao; lực lượng chuyên trách bảo vệ an ninh mạng, phòng chống tội phạm sử dụng công nghệ cao; nâng cao năng lực điều tra số, giám sát an ninh mạng, phân tích mã độc, ứng cứu sự cố và xử lý các tình huống tấn công mạng phức tạp.

- Khuyến khích cán bộ tham gia các chương trình đào tạo, thi lấy chứng chỉ quốc tế uy tín về an ninh mạng; lựa chọn, bồi dưỡng đội ngũ cán bộ có năng lực

nổi trội để xây dựng lực lượng chuyên gia nòng cốt của tỉnh trong các lĩnh vực công nghệ mới như trí tuệ nhân tạo (AI), dữ liệu lớn (Big Data), chuỗi khối (Blockchain), điện toán đám mây, mật mã hiện đại.

- Đẩy mạnh công tác tuyên truyền, phổ biến kiến thức an ninh mạng cho Nhân dân thông qua các nền tảng số, hệ thống truyền thông cơ sở, các chương trình “Bình dân học vụ số”, diễn đàn, hội thi, câu lạc bộ công nghệ; góp phần nâng cao nhận thức, kỹ năng tự bảo vệ của người dân trên không gian mạng.

4. Tăng cường giám sát, chia sẻ thông tin và nâng cao năng lực phòng ngừa, ứng phó sự cố an ninh mạng

- Tổ chức triển khai đồng bộ các giải pháp giám sát, cảnh báo sớm nguy cơ mất an ninh mạng đối với hệ thống thông tin của các cơ quan nhà nước trên địa bàn tỉnh; thường xuyên rà soát, kiểm tra, đánh giá an toàn thông tin đối với các hệ thống thông tin quan trọng phục vụ chỉ đạo, điều hành, cung cấp dịch vụ công và chuyển đổi số.

- Đẩy mạnh xây dựng cơ chế chia sẻ, trao đổi thông tin về nguy cơ, lỗ hổng bảo mật, mã độc, phương thức, thủ đoạn tấn công mạng giữa các cơ quan, đơn vị; nâng cao hiệu quả phối hợp xử lý sự cố, không để xảy ra tình trạng bị động, bất ngờ.

- Tăng cường tổ chức kiểm tra, đánh giá định kỳ mức độ an toàn, an ninh mạng đối với các hệ thống thông tin theo cấp độ; kịp thời khắc phục các tồn tại, hạn chế, điểm yếu bảo mật, bảo đảm hệ thống hoạt động ổn định, liên tục, an toàn.

- Hằng năm tổ chức ít nhất 01 cuộc diễn tập chuyên đề về an ninh mạng và ứng cứu sự cố mạng cấp tỉnh; đồng thời phối hợp tham gia các cuộc diễn tập quốc gia, khu vực và quốc tế nhằm nâng cao khả năng phối hợp tác chiến mạng, xử lý tình huống thực tiễn và nâng cao trình độ chuyên môn cho lực lượng chuyên trách.

- Từng bước xây dựng cơ sở dữ liệu phục vụ công tác giám sát, phân tích, cảnh báo nguy cơ an ninh mạng; bảo đảm dữ liệu “đúng, đủ, sạch, sống, dùng chung và thống nhất”, phục vụ hiệu quả công tác quản lý nhà nước và bảo vệ không gian mạng.

5. Thúc đẩy nghiên cứu, ứng dụng khoa học công nghệ, phát triển hệ sinh thái an ninh mạng “Make in Vietnam”

- Khuyến khích nghiên cứu, ứng dụng các công nghệ mới, công nghệ chiến lược vào công tác quản lý, giám sát và bảo vệ hệ thống thông tin; từng bước nâng cao năng lực tự chủ công nghệ trong lĩnh vực an ninh mạng.

- Ưu tiên sử dụng các sản phẩm, giải pháp, dịch vụ an ninh mạng do doanh nghiệp Việt Nam nghiên cứu, phát triển và làm chủ công nghệ trong các cơ quan nhà nước của tỉnh; góp phần thúc đẩy phát triển ngành công nghiệp an ninh mạng nội địa.

- Tạo điều kiện cho doanh nghiệp công nghệ số, doanh nghiệp khởi nghiệp đổi mới sáng tạo tham gia nghiên cứu, cung cấp giải pháp bảo đảm an ninh mạng phục vụ hoạt động chuyển đổi số, chính quyền số, đô thị thông minh, kinh tế số và xã hội số.

- Đẩy mạnh liên kết giữa cơ quan nhà nước, cơ sở đào tạo, viện nghiên cứu và doanh nghiệp để hình thành hệ sinh thái an ninh mạng bền vững; thúc đẩy hợp tác công - tư trong nghiên cứu, phát triển và chuyển giao công nghệ.

6. Tăng cường hợp tác, nâng cao vị thế và uy tín trong lĩnh vực an ninh mạng

- Chủ động mở rộng hợp tác với các bộ, ngành Trung ương, các địa phương, doanh nghiệp công nghệ và các tổ chức trong nước, quốc tế nhằm trao đổi kinh nghiệm, chia sẻ thông tin, hỗ trợ kỹ thuật và đào tạo nguồn nhân lực về an ninh mạng.

- Tăng cường tham gia các hội nghị, hội thảo, diễn đàn chuyên ngành về an ninh mạng trong nước và quốc tế để cập nhật xu hướng công nghệ, phương thức, thủ đoạn tấn công mạng mới; đồng thời quảng bá hình ảnh địa phương chủ động, trách nhiệm trong công tác bảo đảm an ninh mạng.

- Khuyến khích các cơ quan, doanh nghiệp, chuyên gia công nghệ trên địa bàn tỉnh tham gia các cuộc thi, diễn đàn, chương trình hợp tác quốc tế về an ninh mạng; thúc đẩy giao lưu, học hỏi và tiếp cận các tiêu chuẩn, mô hình tiên tiến trên thế giới.

7. Bảo đảm nguồn lực triển khai thực hiện Đề án

- Ưu tiên bố trí nguồn lực về nhân lực, kinh phí và trang thiết bị phục vụ công tác bảo đảm an ninh mạng tại các cơ quan, đơn vị, địa phương; bảo đảm phù hợp với yêu cầu nhiệm vụ và khả năng cân đối ngân sách của tỉnh.

- Tăng cường huy động nguồn lực xã hội hóa, thúc đẩy sự tham gia của doanh nghiệp, tổ chức, cá nhân trong công tác bảo đảm an ninh mạng; phát huy sức mạnh tổng hợp của cả hệ thống chính trị và toàn xã hội trong bảo vệ chủ quyền, lợi ích quốc gia trên không gian mạng.

III. TỔ CHỨC THỰC HIỆN

1. Công an tỉnh

- Là cơ quan thường trực tham mưu Ủy ban nhân dân tỉnh tổ chức triển khai thực hiện toàn diện Kế hoạch; chủ trì hướng dẫn, kiểm tra, đôn đốc các sở, ngành, địa phương thực hiện các nhiệm vụ bảo vệ an ninh mạng theo quy định.

- Chủ động nắm chắc tình hình an ninh mạng trên địa bàn; kịp thời tham mưu Tỉnh ủy, Ủy ban nhân dân tỉnh, Tiểu ban An ninh mạng tỉnh chỉ đạo xử lý các vấn đề phức tạp phát sinh liên quan an ninh quốc gia, trật tự an toàn xã hội trên không gian mạng.

- Chủ trì xây dựng phương án tổng thể bảo vệ an ninh mạng đối với các hệ thống thông tin trọng yếu của tỉnh; phối hợp tổ chức đánh giá nguy cơ mất an ninh mạng, kiểm tra an toàn thông tin mạng định kỳ đối với hệ thống thông tin thuộc cơ quan Nhà nước.

- Tăng cường công tác nghiệp vụ nhằm phát hiện, đấu tranh, xử lý các loại tội phạm sử dụng công nghệ cao; tập trung đấu tranh với các hành vi: Lừa đảo chiếm đoạt tài sản trên không gian mạng; Tổ chức đánh bạc, đánh bạc trực tuyến; Mua bán dữ liệu cá nhân; Xâm nhập trái phép hệ thống thông tin; Phát tán mã độc, mã hóa dữ liệu tổng tiền; Sử dụng không gian mạng để chống phá Đảng, Nhà nước.

- Chủ trì tham mưu tổ chức các cuộc diễn tập thực chiến an ninh mạng cấp tỉnh; xây dựng phương án ứng phó, xử lý tình huống tấn công mạng quy mô lớn đối với hệ thống thông tin trọng yếu.

- Chủ trì phối hợp với các sở, ngành xây dựng cơ chế chia sẻ dữ liệu, cảnh báo sớm nguy cơ mất an ninh mạng; nâng cao hiệu quả phối hợp liên ngành trong công tác bảo vệ an ninh mạng.

- Chủ trì tổ chức tập huấn, bồi dưỡng kiến thức, kỹ năng an ninh mạng cho cán bộ chuyên trách công nghệ thông tin, cán bộ quản trị hệ thống của các cơ quan, đơn vị.

- Phối hợp các cơ quan báo chí, truyền thông tăng cường tuyên truyền, định hướng dư luận, phản bác thông tin xấu độc, sai sự thật trên không gian mạng.

- Định kỳ sơ kết, tổng kết, đánh giá kết quả triển khai thực hiện; tham mưu Ủy ban nhân dân tỉnh báo cáo Bộ Công an, Chính phủ theo quy định.

2. Sở Khoa học và Công nghệ

- Phối hợp Công an tỉnh và các cơ quan có liên quan nghiên cứu, đề xuất triển khai các giải pháp khoa học, công nghệ, chuyển đổi số theo chức năng, nhiệm vụ được giao.

- Phối hợp Công an tỉnh nghiên cứu, đề xuất ứng dụng công nghệ mới như trí tuệ nhân tạo (AI), dữ liệu lớn (Big Data), điện toán đám mây, phân tích dữ liệu phục vụ công tác giám sát, phát hiện nguy cơ tấn công mạng.

- Phối hợp Công an tỉnh và các cơ quan có liên quan trong việc triển khai các tiêu chuẩn, quy chuẩn kỹ thuật, giải pháp công nghệ phục vụ bảo đảm an ninh mạng, an toàn hệ thống thông tin theo quy định.

- Tham mưu triển khai các nhiệm vụ nghiên cứu, chuyển giao khoa học, công nghệ, chuyển đổi số và đổi mới, sáng tạo; khuyến khích doanh nghiệp công nghệ số trên địa bàn tham gia phát triển sản phẩm, giải pháp an toàn thông tin, bảo đảm phù hợp với chức năng, nhiệm vụ được giao.

- Phối hợp Công an tỉnh, các cơ quan, đơn vị liên quan thúc đẩy hoạt động nghiên cứu khoa học, đổi mới sáng tạo, đào tạo nguồn nhân lực chất lượng cao trong lĩnh vực công nghệ số, phục vụ chuyển đổi số và công tác bảo đảm an ninh mạng.

3. Sở Tài chính

Trên cơ sở số liệu tổng hợp dự toán và đề nghị của Công an tỉnh; căn cứ vào khả năng cân đối ngân sách và chế độ định mức do Nhà nước ban hành, Sở Tài chính phối hợp với Công an tỉnh và các cơ quan, đơn vị có liên quan rà soát phù hợp với tình hình thực tiễn địa phương để tham mưu Ủy ban nhân dân tỉnh nguồn kinh phí thực hiện Kế hoạch đảm bảo theo quy định và phân cấp Luật Ngân sách Nhà nước, các văn bản hướng dẫn có liên quan.

4. Sở Nội vụ

- Chủ trì tham mưu xây dựng cơ chế thu hút, đào tạo, bồi dưỡng nguồn nhân lực chất lượng cao trong lĩnh vực công nghệ thông tin, an ninh mạng.

- Phối hợp tham mưu đưa nội dung bảo đảm an ninh mạng, an toàn thông tin vào chương trình đào tạo, bồi dưỡng cán bộ, công chức, viên chức; tham mưu xây dựng tiêu chí đánh giá trách nhiệm người đứng đầu cơ quan, đơn vị trong thực hiện nhiệm vụ bảo đảm an ninh mạng.

5. Sở Giáo dục và Đào tạo

- Chỉ đạo các cơ sở giáo dục tăng cường tuyên truyền, giáo dục kỹ năng sử dụng Internet an toàn, phòng chống lừa đảo trực tuyến, bạo lực mạng và các hành vi vi phạm pháp luật trên không gian mạng cho học sinh, học viên.

- Phối hợp lực lượng Công an tổ chức các hoạt động ngoại khóa, chuyên đề tuyên truyền pháp luật về an ninh mạng trong trường học.

- Chỉ đạo bảo đảm an toàn thông tin đối với hệ thống cơ sở dữ liệu ngành giáo dục, nền tảng dạy học trực tuyến và hệ thống quản lý học sinh.

6. Sở Văn hóa và Thể thao

- Phối hợp Công an tỉnh tăng cường quản lý thông tin trên không gian mạng thuộc lĩnh vực văn hóa, báo chí, truyền thông, quảng cáo và hoạt động dịch vụ Internet công cộng.

- Chủ động phát hiện, phối hợp xử lý các thông tin xấu độc, thông tin giả, xuyên tạc lịch sử, xúc phạm danh dự tổ chức, cá nhân trên không gian mạng. Đẩy mạnh tuyên truyền xây dựng môi trường văn hóa số lành mạnh, an toàn.

7. Bộ Chỉ huy Quân sự tỉnh

- Phối hợp Công an tỉnh bảo vệ chủ quyền quốc gia trên không gian mạng; chủ động phòng ngừa, phát hiện hoạt động sử dụng không gian mạng xâm phạm quốc phòng, an ninh.

- Phối hợp triển khai các phương án bảo vệ hệ thống thông tin quân sự, quốc phòng trên địa bàn tỉnh. Tham gia diễn tập phòng thủ không gian mạng, ứng phó tình huống tấn công mạng ảnh hưởng quốc phòng - an ninh.

- Chỉ đạo lực lượng Biên phòng chủ động nắm tình hình trên không gian mạng liên quan khu vực biên giới; phối hợp đấu tranh với các đối tượng sử dụng công nghệ cao hoạt động xuyên biên giới. Phối hợp kiểm soát, phát hiện các hành vi sử dụng mạng Internet phục vụ xuất nhập cảnh trái phép, buôn lậu, mua bán người, lừa đảo xuyên quốc gia. Tăng cường phối hợp trao đổi thông tin với lực lượng chức năng Campuchia trong phòng ngừa, đấu tranh tội phạm công nghệ cao khu vực biên giới.

8. Ngân hàng Nhà nước Chi nhánh Khu vực 15

Chỉ đạo các tổ chức tín dụng tăng cường giải pháp bảo mật, bảo đảm an toàn giao dịch điện tử, thanh toán trực tuyến và dữ liệu khách hàng; chủ động phát hiện, cảnh báo giao dịch bất thường, giao dịch có dấu hiệu lừa đảo, rửa tiền qua không gian mạng. Phối hợp Công an tỉnh xác minh, phong tỏa tài khoản, truy vết dòng tiền liên quan hoạt động phạm tội sử dụng công nghệ cao. Đẩy mạnh tuyên truyền cảnh báo thủ đoạn lừa đảo chiếm đoạt tài sản trong lĩnh vực ngân hàng số, thanh toán điện tử.

9. Các doanh nghiệp viễn thông, doanh nghiệp cung cấp dịch vụ Internet

- Tăng cường các biện pháp kỹ thuật bảo đảm an toàn hạ tầng viễn thông, Internet; kịp thời phát hiện, ngăn chặn hoạt động tấn công mạng, phát tán mã độc.

- Thực hiện lưu trữ, cung cấp thông tin phục vụ công tác điều tra, xử lý vi phạm theo quy định pháp luật.

- Phối hợp ngăn chặn thuê bao rác, SIM rác, cuộc gọi rác, tin nhắn rác, website độc hại, ứng dụng giả mạo.

- Chủ động phối hợp lực lượng chức năng xử lý các nền tảng, tài khoản lợi dụng không gian mạng để hoạt động phạm pháp.

10. Ủy ban nhân dân các xã, phường, đặc khu

- Xây dựng kế hoạch cụ thể triển khai thực hiện tại địa phương; xác định công tác bảo vệ an ninh mạng là nhiệm vụ thường xuyên gắn với chuyển đổi số địa phương. Chỉ đạo các phòng, ban chuyên môn rà soát, nâng cao mức độ an toàn hệ thống thông tin phục vụ điều hành, giải quyết thủ tục hành chính.

- Tăng cường tuyên truyền nâng cao nhận thức cho cán bộ, công chức và Nhân dân về phòng chống tội phạm công nghệ cao. Chủ động phối hợp Công an tỉnh xử lý các vụ việc phát sinh liên quan an ninh mạng trên địa bàn.

- Định kỳ tổ chức kiểm tra, đánh giá công tác bảo đảm an ninh mạng tại các cơ quan, đơn vị trực thuộc.

Yêu cầu thủ trưởng các cơ quan, đơn vị, địa phương nghiêm túc quán triệt, triển khai và xây dựng kế hoạch cụ thể hóa nhiệm vụ được giao để tổ chức thực hiện; định kỳ hằng năm hoặc đột xuất tổng hợp báo cáo Ủy ban nhân dân tỉnh kết quả thực hiện (*qua Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh, địa chỉ 368 Trần Văn Giàu, phường Rạch Giá, tỉnh An Giang*). Trong quá trình thực hiện, có phát sinh khó khăn, vướng mắc, báo cáo bằng văn bản về Công an tỉnh để tổng hợp, đề xuất Ủy ban nhân dân tỉnh xem xét, giải quyết./.

Nơi nhận:

- Bộ Công an (để b/c);
- Văn phòng Chính phủ (để b/c);
- Thường trực Tỉnh ủy (để b/c);
- CT và các PCT UBND tỉnh;
- Các sở, ban, ngành và đoàn thể tỉnh;
- Lãnh đạo VP UBND tỉnh;
- UBND xã, phường, đặc khu;
- VNPT An Giang;
- Viettel An Giang;
- Các DN quản lý, kinh doanh Internet trên địa bàn tỉnh;
- Phòng KGVX;
- Lưu: VT, ntgiang.

**KT. CHỦ TỊCH
PHÓ CHỦ TỊCH**

Nguyễn Thanh Phong