TỈNH ỦY AN GIANG	**ĐẢNG CỘNG SẢN VIỆT NAM**
*	*An Giang, ngày 24 tháng 6 năm 2026*
Số 28-CTr/TU	

CHƯƠNG TRÌNH HÀNH ĐỘNG

CỦA BAN THƯỜNG VỤ TỈNH ỦY

thực hiện Chỉ thị số 57-CT/TW, ngày 31/12/2025 của Ban Bí thư Trung ương Đảng về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị

Thực hiện Chỉ thị số 57-CT/TW, ngày 31/12/2025 của Ban Bí thư Trung ương Đảng về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị *(gọi tắt là Chỉ thị số 57-CT/TW),* Ban Thường vụ Tỉnh ủy ban hành Chương trình hành động thực hiện như sau:

I- TÌNH HÌNH VÀ NGUYÊN NHÂN

Những năm qua, thực hiện chủ trương, chỉ đạo của Trung ương về công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu, tỉnh An Giang đã quan tâm lãnh đạo, chỉ đạo, đạt những kết quả bước đầu đáng ghi nhận. Các hệ thống thông tin phục vụ chỉ đạo, điều hành từng bước được triển khai, các giải pháp bảo mật cơ bản được áp dụng; nhận thức của cán bộ, đảng viên, công chức có chuyển biến tích cực; năng lực kỹ thuật bảo đảm an ninh mạng của một số cơ quan được tăng cường. *Tuy nhiên,* hạ tầng kỹ thuật chưa đồng bộ; tỷ lệ hệ thống thông tin được phê duyệt cấp độ an toàn thấp; năng lực giám sát, cảnh báo, ứng cứu sự cố hạn chế chưa theo kịp yêu cầu thực tiễn; dữ liệu chưa được quản trị thống nhất, còn phân tán, thiếu liên thông; nguồn nhân lực chuyên trách về an ninh mạng thiếu, chưa đáp ứng yêu cầu trong tình hình mới. *Những hạn chế* có nguyên nhân khách quan, song nguyên nhân chủ quan vẫn là do nhận thức của một số cấp ủy, cơ quan, đơn vị, địa phương, nhất là người đứng đầu chưa coi trọng đúng mức vai trò của an ninh mạng, bảo mật thông tin, an ninh dữ liệu, thiếu quyết liệt trong lãnh đạo, chỉ đạo; sự phối hợp giữa các cấp, các ngành từng lúc thiếu chặt chẽ; công tác kiểm tra, giám sát đôn đốc thực thi nhiệm vụ chưa thường xuyên.

II- MỤC ĐÍCH, YÊU CẦU, MỤC TIÊU

1. Mục đích, yêu cầu

- Quán triệt sâu sắc, cụ thể hóa và triển khai thực hiện nghiêm túc nội dung Chỉ thị số 57-CT/TW của Ban Bí thư Trung ương Đảng, gắn với nhiệm vụ Nghị quyết số 57-NQ/TW của Bộ Chính trị về phát triển khoa học, công nghệ, đổi mới sáng tạo

và chuyển đổi số; tạo chuyển biến mạnh mẽ về nhận thức, tinh thần trách nhiệm và hành động của các cấp ủy, chính quyền, Mặt trận Tổ quốc và các tổ chức chính trị - xã hội, cán bộ, đảng viên, công chức, viên chức về ý nghĩa, tầm quan trọng của công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là yêu cầu cấp thiết nhằm kiến tạo một không gian mạng an toàn, tin cậy, thúc đẩy mạnh mẽ sự phát triển khoa học, công nghệ, đổi mới sáng tạo, chuyển đổi số; góp phần phát triển kinh tế - xã hội của địa phương nhanh, bền vững, giữ vững quốc phòng, an ninh.

- Tăng cường sự lãnh đạo, chỉ đạo của các cấp ủy, tổ chức đảng, hiệu lực, hiệu quả quản lý của chính quyền, nhất là người đứng đầu; sự phối hợp đồng bộ, chặt chẽ của các ngành, các cấp và hệ thống chính trị, tạo sức mạnh tổng hợp, nâng cao chất lượng, hiệu quả công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu; chủ động sẵn sàng ứng phó với các nguy cơ, thách thức từ không gian mạng. Việc triển khai thực hiện đồng bộ, thống nhất, trọng tâm, tuân thủ đầy đủ các quy định của pháp luật về an ninh mạng, bảo vệ bí mật nhà nước, bảo vệ dữ liệu cá nhân và các tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin.

2. Mục tiêu

Xây dựng không gian mạng của tỉnh an toàn, vững mạnh, có năng lực phòng vệ tốt, khả năng chống chịu cao, bảo vệ vững chắc chủ quyền lãnh thổ, biển đảo, an ninh biên giới quốc gia trên không gian mạng, ổn định chính trị, xã hội. Xây dựng nền an ninh mạng bền vững, tự chủ, có năng lực cạnh tranh cao. Phát triển hạ tầng an ninh mạng, hạ tầng số hiện đại, góp phần phát triển chính quyền số, kinh tế số, xã hội số, công dân số; đưa An Giang thuộc nhóm các tỉnh, thành phố dẫn đầu về an toàn, an ninh không gian mạng, an ninh dữ liệu và bảo vệ dữ liệu.

III- NHIỆM VỤ, GIẢI PHÁP CHỦ YẾU

1. Tăng cường sự lãnh đạo của Đảng, nâng cao nhận thức, trách nhiệm của cả hệ thống chính trị và toàn dân về an ninh mạng, bảo mật thông tin, an ninh dữ liệu

- Các cấp ủy, tổ chức đảng, cán bộ, đảng viên trong hệ thống chính trị và toàn xã hội quán triệt sâu sắc, nhận thức đầy đủ, toàn diện Chỉ thị số 57-CT/TW của Ban Bí thư Trung ương Đảng và các chủ trương, chỉ đạo của Trung ương về an ninh mạng, bảo mật thông tin, an ninh dữ liệu; xác định đây là nhiệm vụ trọng yếu, thường xuyên, cấp bách, là trách nhiệm của cả hệ thống chính trị và toàn dân, đặt dưới sự lãnh đạo trực tiếp, toàn diện của Đảng, sự quản lý tập trung, thống nhất của Nhà nước.

- Đổi mới tư duy, nâng cao nhận thức, gắn trách nhiệm người đứng đầu trong triển khai thực hiện nhiệm vụ, phải trực tiếp phụ trách, chỉ đạo toàn diện, xác định rõ những vấn đề trọng tâm, trọng điểm để chỉ đạo; cán bộ, đảng viên phải gương

mẫu thực hiện nghiêm túc, hiệu quả công tác bảo đảm an ninh mạng, an ninh dữ liệu, bảo vệ bí mật nhà nước tại địa phương, đơn vị mình quản lý. Kết quả công tác này là một trong những tiêu chí quan trọng để đánh giá, xếp loại tổ chức, cán bộ, đảng viên, công chức, viên chức và người lao động hằng năm. Lực lượng Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, Văn phòng Tỉnh ủy, Văn phòng Ủy ban nhân dân tỉnh, Sở Khoa học và Công nghệ đóng vai trò nòng cốt.

- Huy động sức mạnh tổng hợp của toàn dân, xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng. Phát huy sự tham gia hiệu quả của các tầng lớp nhân dân trong công tác bảo đảm an toàn, an ninh mạng và chủ động ứng phó với các nguy cơ, thách thức từ không gian mạng. Hình thành thế trận an ninh nhân dân trên không gian mạng kết hợp chặt chẽ với thế trận quốc phòng toàn dân trên không gian mạng. Xây dựng cơ chế hợp tác giữa các cơ quan Đảng, Nhà nước, các doanh nghiệp, hiệp hội doanh nghiệp trên địa bàn tỉnh trong xây dựng và thực thi các chính sách về an toàn, an ninh mạng.

- Chuyển dịch tư duy chiến lược từ "Phòng thủ bị động" sang "Phòng thủ chủ động", "Phòng thủ tích cực", xây dựng "Thế trận an ninh mạng chủ động, toàn diện"; những nguy cơ, thách thức về an ninh mạng, bảo mật thông tin, an ninh dữ liệu phải được nhận diện và xử lý từ sớm, từ xa, sẵn sàng các biện pháp phòng vệ tương xứng để răn đe, vô hiệu hoá các nguy cơ, bảo vệ lợi ích quốc gia - dân tộc.

- Quán triệt phương châm "Tự chủ, tự lực, tự cường" trong xây dựng tiềm lực an ninh mạng. Vận dụng, khai thác, sử dụng hiệu quả hệ sinh thái sản phẩm, dịch vụ an ninh mạng Việt Nam, ưu tiên làm chủ công nghệ lõi, giải pháp bảo mật tiên tiến, ứng dụng mạnh mẽ trí tuệ nhân tạo, công nghệ mới vào lĩnh vực an ninh mạng theo chỉ đạo, hướng dẫn của Trung ương, coi đây là những nhiệm vụ chiến lược để bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng. Áp dụng cơ chế đột phá, đặc thù, ưu đãi nhất trong lĩnh vực khoa học, công nghệ, đổi mới sáng tạo để phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng, an ninh dữ liệu.

- Bảo đảm an ninh mạng, an ninh dữ liệu là yếu tố nền tảng, yêu cầu bắt buộc ngay từ khâu quy hoạch, thiết kế, xây dựng, vận hành hệ thống thông tin. Hệ thống chưa bảo đảm an toàn, an ninh thì kiên quyết chưa đưa vào sử dụng. Thường xuyên rà soát, kiểm tra, đánh giá an ninh mạng đối với các hệ thống công nghệ thông tin trên địa bàn tỉnh. Việc thu thập, quản lý, khai thác dữ liệu số phải được bảo vệ ở mức độ cao nhất; tuyệt đối không để lộ, lọt bí mật nhà nước, dữ liệu nhạy cảm, kể cả trong quá trình thử nghiệm.

- Đổi mới mạnh mẽ nội dung, hình thức tuyên truyền, giáo dục kiến thức, kỹ năng an ninh mạng; đưa nội dung này vào chương trình của hệ thống giáo dục quốc dân, chuyên đề trong Phong trào "Bình dân học vụ số" để xây dựng "thế hệ công dân số" văn minh, tuân thủ pháp luật. Tham gia, phối hợp triển khai đánh giá tín

nhiệm mạng, phát triển cơ chế liên kết và hợp tác nhằm xây dựng một không gian mạng an toàn, tin cậy, thúc đẩy các giá trị nhân văn và nâng cao ý thức trách nhiệm bảo đảm an ninh không gian mạng đến mọi người dùng; phát động phong trào toàn dân bảo vệ an ninh mạng; phát huy trách nhiệm xã hội của cơ quan báo chí và người có uy tín trong việc định hướng dư luận, lan tỏa thông tin tích cực và đấu tranh với các thông tin xấu độc. Tập trung đào tạo, nâng cao năng lực, kỹ năng của lực lượng chuyên trách về an ninh mạng.

- Tham gia, phối hợp triển khai hệ thống định danh và xác thực không gian mạng quốc gia; thống nhất định danh công dân, người dùng mạng xã hội, thuê bao viễn thông và tài nguyên Internet (tên miền, địa chỉ IP...). Kiên quyết xử lý triệt để tình trạng SIM "rác", tài khoản "ảo", nặc danh; áp dụng biện pháp xác thực danh tính bắt buộc đối với người dùng mạng xã hội và cơ chế kiểm soát độ tuổi để bảo vệ trẻ em trên không gian mạng.

2. Hoàn thiện thể chế, chính sách và nâng cao hiệu lực, hiệu quả quản lý nhà nước

- Tiếp tục thể chế hóa đầy đủ, kịp thời và thực hiện có hiệu quả các chủ trương, chính sách của Đảng, pháp luật của Nhà nước về bảo đảm an toàn, an ninh mạng, bảo mật thông tin, bảo vệ dữ liệu cá nhân, dữ liệu quốc gia, tiêu chuẩn, quy chuẩn kỹ thuật. Thực hiện rà soát, đề xuất xây dựng, sửa đổi, bổ sung, hoàn thiện đồng bộ các quy định, quy chế, chính sách về bảo đảm an toàn, an ninh mạng cho giao dịch điện tử, chuyển đổi số, hạ tầng số, nền tảng số, bảo vệ thông tin cá nhân, chế tài xử lý các hành vi vi phạm pháp luật trên không gian mạng... theo quy định pháp luật và phù hợp tình hình địa phương.

- Thống nhất đầu mối, phân định rõ trách nhiệm quản lý nhà nước bảo đảm hiệu lực, hiệu quả. Trong đó:

Về an ninh mạng: Công an tỉnh chịu trách nhiệm trước Ban Thường vụ Tỉnh ủy chủ trì quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu xuyên suốt đối với các hệ thống thông tin, cơ sở dữ liệu của toàn hệ thống chính trị trên địa bàn tỉnh và quản lý hoạt động cung cấp sản phẩm, dịch vụ an ninh mạng đối với các hệ thống này *(trừ hệ thống thông tin, cơ sở dữ liệu quân sự và cơ yếu trong phạm vi Bộ Chỉ huy Quân sự tỉnh quản lý).*

Về mật mã và sản phẩm mật mã: Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh, Văn phòng Tỉnh ủy, Ủy ban nhân dân tỉnh thực hiện trách nhiệm, phạm vi quản lý theo đúng quy định tại Luật An ninh mạng năm 2025.

- Thực hiện nghiêm quy định pháp luật yêu cầu hồ sơ thiết kế hệ thống thông tin, dự án chuyển đổi số trên địa bàn tỉnh phải có cấu phần an ninh mạng được thẩm định, phê duyệt trước khi đầu tư xây dựng.

- Chuyển đổi tư duy từ quản lý kỹ thuật thuần túy sang quản trị rủi ro toàn diện nhằm tăng tính chủ động phân bổ nguồn lực và giảm thiểu tổn thất. Áp dụng có hiệu quả Bộ chỉ số đánh giá năng lực bảo đảm an ninh mạng để xếp hạng các sở, ban, ngành, địa phương, tổ chức. Có cơ chế trao đổi, chia sẻ thông tin và quy trình phối hợp ứng cứu sự cố giữa các cơ quan, tổ chức trên địa bàn tỉnh.

- Quản lý chặt chẽ hoạt động của các doanh nghiệp cung cấp dịch vụ trên không gian mạng trên địa bàn tỉnh (bao gồm cả dịch vụ xuyên biên giới). Quy định rõ trách nhiệm của các doanh nghiệp viễn thông, Internet, tài chính, ngân hàng đóng trên địa bàn tỉnh trong việc bảo đảm an ninh hệ thống và phối hợp với cơ quan chức năng (Công an tỉnh, Bộ Chỉ huy Quân sự tỉnh); thiết lập cơ chế kết nối kỹ thuật, cung cấp dữ liệu, chứng cứ điện tử nhanh chóng, kịp thời, bảo đảm "đúng, đủ, sạch, sống" để phục vụ công tác điều tra, xử lý tội phạm và bảo vệ chủ quyền quốc gia; đơn giản hóa thủ tục hành chính trong các tình huống khẩn cấp về an ninh mạng.

3. Tập trung đầu tư, hiện đại hóa hạ tầng, công nghệ và các giải pháp kỹ thuật bảo đảm an ninh mạng

- Nâng cao trách nhiệm bảo vệ hệ thống thông tin thuộc phạm vi quản lý; gắn trách nhiệm của người đứng đầu cơ quan chủ quản hệ thống thông tin với công tác bảo đảm an toàn, an ninh mạng. Vận hành hệ thống thông tin theo tiêu chuẩn, quy chuẩn kỹ thuật về an toàn, an ninh mạng. Thực hiện rà soát, lập hồ sơ đề nghị đưa các hệ thống thông tin trọng yếu, phù hợp với quy định của pháp luật vào danh mục hệ thống thông tin quan trọng về an ninh mạng quốc gia (nếu có).

- Thực hiện nghiêm các quy định pháp luật về bảo vệ an ninh mạng; xác định cấp độ và triển khai mô hình bảo vệ 4 lớp trước khi đưa vào sử dụng, nhất là hệ thống thông tin của các lĩnh vực quan trọng cần ưu tiên bảo đảm an toàn thông tin. Chủ động giám sát, kịp thời phát hiện nguy cơ mất an toàn, an ninh mạng trong quá trình thi công, lắp đặt thiết bị trong các hệ thống thông tin. Ưu tiên sử dụng sản phẩm, giải pháp an toàn, an ninh mạng "Made in Vietnam". Khuyến khích xã hội hoá đối với công tác phát triển, ứng dụng sản phẩm mật mã dân sự để bảo mật thông tin.

- Đầu tư có trọng tâm, trọng điểm việc nâng cấp hệ thống, cập nhật bản quyền, đào tạo nâng cao nhận thức, kỹ năng an toàn, an ninh mạng cho cán bộ, đảng viên, người lao động. Tổ chức diễn tập, hướng dẫn, kiểm tra, ứng phó và ứng cứu sự cố an toàn, an ninh mạng. Sử dụng các giải pháp dùng mật mã để bảo vệ thông tin trong hệ thống thông tin của đơn vị theo quy định.

- Phối hợp vận hành hiệu quả Hệ thống phòng vệ mạng quốc gia, nền tảng điều hành an ninh mạng quốc gia và các nền tảng số dùng chung quốc gia chuyên ngành an ninh mạng là nền tảng dùng chung trong khung kiến trúc tổng thể quốc gia số, nhằm bảo vệ an ninh mạng cho các hệ thống thông tin, tài nguyên trọng yếu trên

Internet của các sở, ban, ngành, địa phương, cơ quan, doanh nghiệp trên địa bàn tỉnh; có khả năng tích hợp, kết nối với các sản phẩm an ninh mạng phù hợp, đáp ứng tiêu chuẩn, quy chuẩn về an ninh mạng. Tập trung xây dựng, nâng cao năng lực quản lý, vận hành hiệu quả Trung tâm an ninh mạng tỉnh (SOC) theo quy định. Mở rộng kết nối giám sát an ninh mạng đến toàn bộ cơ sở dữ liệu dùng chung, cơ sở dữ liệu chuyên ngành, hệ thống thông tin, hệ thống dùng chung của toàn hệ thống chính trị trên địa bàn tỉnh. Đôn đốc các cơ quan, đơn vị, địa phương thiết lập kênh kết nối trao đổi thông tin, dữ liệu phục vụ giám sát, điều phối ứng cứu, khắc phục sự cố an ninh mạng theo hướng dẫn của lực lượng chuyên trách.

- Tổ chức rà soát, kiểm tra, đánh giá định kỳ công tác bảo đảm an ninh thông tin, an ninh mạng. Tăng cường phối hợp chặt chẽ, hiệp đồng tác chiến giữa các lực lượng chuyên trách trong bảo vệ an ninh mạng toàn hệ thống chính trị.

- Rà soát, điều chỉnh quy hoạch hạ tầng công nghệ thông tin theo hướng tập trung máy chủ về các trung tâm dữ liệu đạt chuẩn, đủ điều kiện an ninh mạng. Tăng cường bảo đảm an ninh kết nối, duy trì sự ổn định, thông suốt và an toàn của các luồng dữ liệu, kết nối trong mọi tình huống, không để xảy ra bị động, bất ngờ.

- Bảo đảm nguồn lực tài chính bền vững cho công tác an ninh mạng. Thực hiện nghiêm quy định ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng trong nước trong các dự án đầu tư công của tỉnh. Bảo đảm tỷ lệ kinh phí chi cho an ninh mạng, bảo mật thông tin đạt tối thiểu 15% tổng kinh phí triển khai kế hoạch ứng dụng công nghệ thông tin, chuyển đổi số.

4. Xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng; phát triển tiềm lực, công nghệ và nguồn nhân lực

- Xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng vững chắc. Phát huy vai trò nòng cốt của lực lượng vũ trang nhân dân; huy động sức mạnh tổng hợp của các doanh nghiệp công nghệ, viễn thông và các tầng lớp nhân dân trên địa bàn tỉnh. Các doanh nghiệp cung cấp dịch vụ viễn thông, Internet phải xác định rõ trách nhiệm là "tuyến đầu" trong bảo vệ an ninh mạng.

- Chú trọng vận hành, làm chủ các sản phẩm cốt lõi, nền tảng bao gồm: Giải pháp tường lửa, phòng, chống mã độc, bảo vệ thiết bị đầu cuối, nền tảng điện toán đám mây và hệ điều hành dùng riêng. Có cơ chế, chính sách hỗ trợ, thu hút, khuyến khích doanh nghiệp công nghệ, cộng đồng khởi nghiệp sáng tạo tham gia phát triển hệ sinh thái an ninh mạng.

- Đẩy mạnh đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao. Tăng cường liên kết giữa Nhà nước - Nhà trường - Doanh nghiệp trong đào tạo, huấn luyện thực chiến. Xây dựng mạng lưới chuyên gia an ninh mạng trên địa bàn tỉnh, sẵn sàng huy động nguồn lực xã hội tham gia ứng cứu sự cố, tình huống nguy hiểm

về an ninh mạng. Tiếp tục hoàn thiện cơ chế, chính sách thu hút, đãi ngộ chuyên gia giỏi, nhân tài tham gia phục vụ công tác an ninh mạng trên địa bàn tỉnh.

5. Tăng cường hợp tác quốc tế trên lĩnh vực an ninh mạng

Tăng cường phối hợp tác quốc tế trong phòng, chống và ứng phó sự cố tấn công mạng; điều tra, truy tố tội phạm mạng thường xuyên quốc gia; bảo đảm độc lập, tự chủ, chủ quyền lãnh thổ trong quá trình hợp tác, tiếp thu kinh nghiệm, công nghệ, chuẩn mực quốc tế về an ninh mạng; tạo điều kiện cho cán bộ tham gia đào tạo, huấn luyện chuyên sâu tại nước ngoài và tích cực tham gia các cuộc diễn tập an ninh mạng quốc tế.

IV- TỔ CHỨC THỰC HIỆN

1. Rà soát, kiện toàn, nâng cao chất lượng Tiểu ban An ninh mạng tỉnh, do đồng chí Bí thư Tỉnh ủy làm Trưởng Tiểu ban; lãnh đạo, chỉ đạo, tổ chức thực hiện Chỉ thị 57-CT/TW của Ban Bí thư Trung ương Đảng và Chương trình hành động này.

2. Các cấp ủy, tổ chức đảng trực thuộc Tỉnh ủy, các sở, ngành, Mặt trận Tổ quốc Việt Nam và các tổ chức chính trị - xã hội tỉnh tổ chức nghiên cứu, quán triệt, tuyên truyền, triển khai Chỉ thị 57-CT/TW của Ban Bí thư Trung ương Đảng và Chương trình hành động của Ban Thường vụ Tỉnh ủy đến cán bộ, đảng viên và các tầng lớp nhân dân, nhằm nâng cao nhận thức về vai trò, tầm quan trọng của công tác tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong phát triển kinh tế - xã hội, giữ vững quốc phòng, an ninh của tỉnh; cụ thể hóa kế hoạch triển khai thực hiện phù hợp với chức năng, đặc điểm tình hình của cơ quan, đơn vị, địa phương; chịu trách nhiệm trước Ban Thường vụ Tỉnh ủy về kết quả công tác bảo đảm an ninh mạng tại cơ quan, đơn vị, địa phương quản lý.

3. Đảng ủy Ủy ban nhân dân tỉnh lãnh đạo việc cụ thể hóa kế hoạch thực hiện Chương trình hành động này của Ban Thường vụ Tỉnh ủy. Quá trình tổ chức thực hiện, theo dõi, kịp thời cập nhật, điều chỉnh, có giải pháp thực hiện phù hợp, hiệu quả Chương trình hành động này. Tập trung rà soát, hoàn thiện cơ chế, chính sách, quy định về an ninh mạng, cơ yếu, bảo vệ bí mật nhà nước và các văn bản có liên quan. Thường xuyên kiểm tra, đôn đốc việc triển khai thực hiện, tham mưu cho Ban Thường vụ Tỉnh ủy hằng năm có hình thức cụ thể hóa trong các nghị quyết, kế hoạch phù hợp; định kỳ sơ kết, tổng kết, báo cáo để rút kinh nghiệm chỉ đạo, thực hiện.

4. Đảng ủy Công an tỉnh chịu trách nhiệm trước Ban Thường vụ Tỉnh ủy về công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu của tỉnh (trừ lĩnh vực quân sự, cơ yếu). Lãnh đạo Công an tỉnh chủ trì, phối hợp với các ngành chức năng triển khai nhiệm vụ quản lý nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu và ứng dụng sản phẩm mật mã an ninh theo chỉ đạo của Trung ương, của tỉnh.

5. Đảng ủy Quân sự tỉnh chịu trách nhiệm toàn diện trước Ban Thường vụ Tỉnh ủy về công tác bảo đảm an ninh mạng, mật mã, bảo mật thông tin trong lĩnh vực quân sự, cơ yếu thuộc phạm vi quản lý. Lãnh đạo Bộ Chỉ huy Quân sự tỉnh và Ban Chỉ huy Bộ đội Biên phòng tỉnh tham mưu triển khai thực hiện các nhiệm vụ bảo đảm an ninh mạng, mật mã, bảo mật thông tin trong lĩnh vực quân sự, cơ yếu theo chỉ đạo của Trung ương, của tỉnh.

6. Ban Tuyên giáo và Dân vận Tỉnh ủy chủ trì chỉ đạo, định hướng công tác quán triệt, tuyên truyền sâu rộng thực hiện Chỉ thị 57-CT/TW của Ban Bí thư Trung ương Đảng và Chương trình hành động của Ban Thường vụ Tỉnh ủy trong toàn hệ thống chính trị và các tầng lớp nhân dân.

7. Các cơ quan tham mưu, giúp việc của Tỉnh ủy theo chức năng, nhiệm vụ thường xuyên theo dõi, kiểm tra, giám sát, đôn đốc việc triển khai thực hiện; định kỳ báo cáo Ban Thường vụ Tỉnh ủy (qua Văn phòng Tỉnh ủy) theo quy định.

Chương trình hành động này được phổ biến đến các chi bộ, đảng bộ.

T/M BAN THƯỜNG VỤ
PHÓ BÍ THƯ THƯỜNG TRỰC

ĐẢNG CỘNG SẢN VIỆT NAM
TỈNH ỦY AN GIANG

Nguyễn Thanh Nhàn

Nơi nhận:
- Ban Bí thư Trung ương Đảng (để b/c);
- Văn phòng Trung ương Đảng (để b/c);
- Ban Chỉ đạo Trung ương (để b/c);
- Các đ/c ban đảng Trung ương phụ trách địa bàn;
- Các đ/c Tỉnh ủy viên;
- Các cơ quan tham mưu, giúp việc Tỉnh ủy;
- Các đảng ủy trực thuộc Tỉnh ủy;
- Đảng ủy CQ UBMTTQ và tổ chức CT-XH tỉnh;
- Đảng ủy VP Đoàn ĐBQH và HĐND tỉnh;
- Các sở, ban, ngành tỉnh;
- Lưu Văn phòng Tỉnh ủy.