ỦY BAN NHÂN DÂN XÃ VĨNH THUẬN	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 250 /KH-UBND	*Vĩnh Thuận, ngày 30 tháng 9 năm 2026*

KẾ HOẠCH

Thực hiện Chương trình hành động số 28-CTr/TU, ngày 24/6/2026 của Ban Thường vụ Tỉnh ủy An Giang về 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

Căn cứ Chương trình hành động số 28-CTr/TU, ngày 24/6/2026 của Ban Thường vụ Tỉnh ủy An Giang về 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 Kế hoạch số 104-KH/ĐU ngày 20/8/2026 của Ban Thường vụ Đảng ủy xã Vĩnh Thuận về thực hiện Chương trình hành động số 28-CTr/TU, ngày 24/6/2026 của Ban Thường vụ Tỉnh ủy An Giang về 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. Ủy ban nhân dân xã ban hành kế hoạch triển khai thực hiện, cụ thể như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

- Cụ thể hóa và tổ chức triển khai thực hiện nghiêm túc, đồng bộ, hiệu quả Chỉ thị số 57-CT/TW, Chương trình hành động số 28-CTr/TU và Kế hoạch số 104-KH/ĐU trên địa bàn xã; góp phần bảo vệ vững chắc an ninh quốc gia, bảo vệ nền tảng tư tưởng của Đảng, bảo vệ chủ quyền, lợi ích quốc gia trên không gian mạng.

- Lấy phòng ngừa là chính; nâng cao năng lực phòng ngừa, phát hiện, giám sát, cảnh báo, ứng cứu, xử lý, khắc phục sự cố an ninh mạng; chủ động phòng, chống tấn công mạng, gián điệp mạng, lộ lọt bí mật Nhà nước, dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu nhạy cảm.

- Bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu là nhiệm vụ thường xuyên, liên tục của các cơ quan, đơn vị trong quá trình chuyển đổi số, xây dựng chính quyền số, phát triển kinh tế số, xã hội số; gắn bảo đảm an ninh mạng với cải cách hành chính, Đề án 06, bảo vệ bí mật Nhà nước, bảo đảm quốc phòng, an ninh, trật tự an toàn xã hội và phát triển kinh tế - xã hội của xã. Xác định dữ liệu là tài nguyên quan trọng, nền tảng phục vụ chuyển đổi số, phát triển kinh tế số, xã hội số; bảo đảm quản lý chặt chẽ, an toàn, an ninh đối với dữ liệu trong toàn bộ vòng đời thu thập, lưu trữ, xử lý, kết nối, chia sẻ và khai thác, sử dụng.

- Nâng cao nhận thức, trách nhiệm của các cơ quan, đơn vị nhất là trách nhiệm của người đứng đầu; phát huy vai trò nòng cốt của lực lượng Công an, sự

phối hợp của Ủy ban Mặt trận Tổ quốc Việt Nam, tổ chức chính trị - xã hội, các cơ quan chuyên môn, doanh nghiệp và Nhân dân trong xây dựng thế trận an ninh nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng.

- Từng bước nâng cao năng lực của lực lượng, cán bộ, đầu mối tham gia công tác bảo vệ an ninh mạng tại các cơ quan, đơn vị; tăng cường phối hợp, chia sẻ thông tin, cảnh báo sớm, xử lý kịp thời sự cố, bảo đảm an toàn hệ thống thông tin, cơ sở dữ liệu, nền tảng số.

2. Yêu cầu

- Việc triển khai thực hiện phải bảo đảm đồng bộ, toàn diện, có trọng tâm, trọng điểm; bảo đảm nguyên tắc "06 rõ": Rõ người, rõ việc, rõ trách nhiệm, rõ tiến độ, rõ kết quả, rõ thẩm quyền.

- Bám sát mục tiêu, chỉ tiêu, nhiệm vụ, giải pháp tại Chương trình hành động số 28-CTr/TU của Ban Thường vụ Tỉnh ủy và Kế hoạch số 104-KH/ĐU của Ban Thường vụ Đảng ủy xã; bảo đảm thống nhất, đồng bộ trong tổ chức triển khai thực hiện.

- Phân định rõ trách nhiệm giữa công tác an ninh mạng, an toàn thông tin, chuyển đổi số, bảo vệ bí mật Nhà nước, bảo vệ dữ liệu và các nhiệm vụ liên quan; bảo đảm phối hợp chặt chẽ, thống nhất, đồng bộ trong quá trình tổ chức thực hiện.

- Việc tổ chức thực hiện Kế hoạch phải bảo đảm đồng bộ, hiệu quả, tiết kiệm, phù hợp điều kiện thực tế và khả năng cân đối nguồn lực của xã.

II. MỤC TIÊU

1. Mục tiêu chung

Tăng cường sự lãnh đạo, chỉ đạo và tổ chức thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị của xã; nâng cao hiệu lực, hiệu quả quản lý Nhà nước; xây dựng không gian mạng của xã an toàn, lành mạnh, tin cậy; phục vụ hiệu quả công tác lãnh đạo của Đảng, quản lý, điều hành của chính quyền; góp phần giữ vững an ninh chính trị, trật tự an toàn xã hội, bảo vệ bí mật Nhà nước, bảo đảm quốc phòng, an ninh và thúc đẩy phát triển kinh tế - xã hội của địa phương trong tình hình mới.

2. Mục tiêu đến năm 2030

- Tạo chuyển biến mạnh mẽ về nhận thức, trách nhiệm và hành động của các cơ quan, đơn vị, tổ chức; các cán bộ, công chức, viên chức và Nhân dân về vai trò, ý nghĩa của công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu; xác định đây là nhiệm vụ chủ yếu và thường xuyên.

- Tiếp tục rà soát, đề xuất sửa đổi, bổ sung, hoàn thiện hành lang pháp lý cho an ninh mạng, bảo mật thông tin, an ninh dữ liệu.

- Triển khai các chương trình đào tạo, bồi dưỡng, phổ biến kiến thức an ninh mạng, an toàn thông tin trên nền tảng "Bình dân học vụ số" đến cán bộ, công chức, viên chức trên địa bàn xã (*sau khi có chương trình, khóa học trên nền tảng "Bình dân học vụ số" của Bộ Công an và hướng dẫn của tỉnh*).

- Phối hợp hoàn thiện các cơ sở dữ liệu thuộc phạm vi quản lý đảm bảo kết nối liên thông với hệ thống thông tin, cơ sở dữ liệu quốc gia.

- Phối hợp, triển khai hiệu quả hệ thống định danh và xác thực điện tử; tăng cường quản lý thuê bao viễn thông, tài khoản mạng xã hội; đấu tranh, xử lý tình trạng SIM "rác", tài khoản "ảo", nặc danh, góp phần xây dựng môi trường mạng an toàn, lành mạnh.

- Hình thành cơ chế chia sẻ thông tin, cảnh báo, điều phối ứng phó sự cố giữa lực lượng tham gia bảo vệ an ninh mạng, cơ quan quản lý hệ thống thông tin, doanh nghiệp cung cấp dịch vụ viễn thông phụ trách địa bàn xã.

- Từng bước nâng cao năng lực giám sát, cảnh báo, ứng cứu sự cố an ninh mạng của xã; sẵn sàng kết nối, chia sẻ thông tin với hệ thống giám sát, cảnh báo, điều hành an ninh mạng của Trung ương theo hướng dẫn của Bộ Công an và cơ quan có thẩm quyền.

- Các cơ quan, đơn vị, tổ chức trên địa bàn xã ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng "Made in Vietnam" theo quy định pháp luật, tiêu chuẩn, quy chuẩn kỹ thuật và hướng dẫn của cơ quan có thẩm quyền.

3. Tầm nhìn đến năm 2045

Xây dựng môi trường số an toàn, tin cậy trong hệ thống chính trị; hạ tầng số và các giải pháp bảo đảm an ninh mạng được đầu tư, hoàn thiện đồng bộ, đáp ứng yêu cầu chuyển đổi số và phát triển chính quyền số. Các hoạt động chỉ đạo, điều hành được thực hiện trên nền tảng số an toàn, bảo mật, thông suốt, hiệu quả; dữ liệu được quản lý, khai thác và sử dụng theo đúng quy định, phục vụ kịp thời công tác quản lý, điều hành và cung cấp dịch vụ công, đáp ứng ngày càng tốt hơn nhu cầu của người dân và doanh nghiệp. Đội ngũ cán bộ, công chức, viên chức được trang bị đầy đủ kiến thức, kỹ năng về an ninh mạng, bảo mật thông tin, an ninh dữ liệu; nâng cao năng lực phòng ngừa, phát hiện, ứng phó và xử lý hiệu quả các nguy cơ, sự cố an ninh mạng, góp phần xây dựng hệ thống chính quyền xã trong sạch, vững mạnh, hoạt động an toàn, hiệu lực, hiệu quả trong môi trường số.

III. NHIỆM VỤ, GIẢI PHÁP

1. Nâng cao nhận thức, trách nhiệm của cán bộ, công chức, viên chức, người lao động; quyết liệt trong lãnh đạo, chỉ đạo nhằm bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu

- Tăng cường công tác tuyên truyền, quán triệt Chỉ thị số 57-CT/TW, Chương trình hành động 28-CTr/TU, Kế hoạch số 104-KH/ĐU và nội dung Kế hoạch này đến toàn thể cán bộ, công chức, viên chức, người lao động góp phần nâng cao nhận thức, kỹ năng, trách nhiệm, tạo sự đồng thuận cao trong thực hiện hiệu quả công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu, bảo vệ bí mật Nhà nước tại cơ quan, đơn vị, doanh nghiệp.

- Thủ trưởng các cơ quan, đơn vị xác định nhiệm vụ về bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu, bảo vệ bí mật Nhà nước là nhiệm vụ quan trọng, thường xuyên trong công tác lãnh đạo, chỉ đạo và quản lý, điều hành;

quan tâm công tác xây dựng cán bộ chuyên trách bảo đảm an ninh mạng, công nghệ thông tin; bảo đảm điều kiện cơ sở vật chất phục vụ công tác đảm bảo an ninh mạng, bảo mật thông tin, an ninh dữ liệu; chịu trách nhiệm trực tiếp, toàn diện về 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.

- Triển khai đánh giá tín nhiệm mạng; 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 toả thông tin tích cực và đấu tranh với các thông tin xấu độc.

2. Khẩn trương hoàn thiện, triển khai hiệu quả các thể chế, chính sách và nâng cao hiệu lực, hiệu quả quản lý Nhà nước về an ninh mạng, bảo mật thông tin, an ninh dữ liệu

- Triển khai, áp dụng các thể chế, chính sách pháp luật về công tác bảo đảm an ninh mạng, an toàn thông tin đối với hệ thống thông tin trên địa bàn, gồm: Áp dụng các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật về bảo đảm an ninh mạng; triển khai khung quản lý rủi ro an ninh mạng và chỉ số đánh giá năng lực bảo đảm an ninh mạng của các cơ quan, ban, ngành.

- Quy hoạch và phát triển hạ tầng số, hạ tầng dữ liệu của xã bảo đảm hiện đại, đồng bộ, an toàn. Thực hiện nghiêm quy định pháp luật yêu cầu hồ sơ thiết kế hệ thống thông tin, dự án chuyển đổi số phải có cấu trúc phần an ninh mạng được thẩm định, phê duyệt trước khi đầu tư xây dựng.

- Phối hợp các doanh nghiệp viễn thông, Internet, tài chính, ngân hàng trong việc bảo đảm an ninh hệ thống; phối hợp thiết lập cơ chế 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 hoá 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; giải pháp kỹ thuật bảo đảm an ninh mạng và năng lực ứng cứu sự cố an ninh mạng

- Áp dụng đồng bộ kiến trúc bảo vệ an ninh mạng theo hướng dẫn của tỉnh cho hạ tầng mạng Internet và hệ thống thông tin của các cơ quan, đơn vị, tổ chức trên địa bàn xã. Phối hợp khảo sát, kết nối các hệ thống thông tin quan trọng trên địa bàn tới Hệ thống phòng vệ mạng quốc gia, Nền tảng điều hành an ninh mạng quốc gia, Trung tâm An ninh mạng quốc gia.

- Phối hợp với các cơ quan chuyên môn cấp tỉnh rà soát 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 của tỉnh. Tăng cường bảo đảm an ninh kết nối, duy trì sự ổn định, thông suốt và an toàn an ninh mạng. Xây dựng hạ tầng công nghệ số hiện đại, an toàn và đồng bộ, đáp ứng yêu cầu phát triển kinh tế - xã hội và chuyển đổi số; xây dựng hệ thống bảo vệ dữ liệu và không gian mạng an toàn.

- Xác định, đề xuất tỉnh phê duyệt cấp độ an toàn thông tin đối với các hệ

thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý; triển khai đầy đủ các phương án bảo đảm an toàn thông tin theo hồ sơ đề xuất đã được phê duyệt.

- Triển khai mô hình bảo đảm an toàn thông tin 04 lớp đối với hệ thống thông tin quan trọng, gồm: Lực lượng tại chỗ; hệ thống hoặc dịch vụ giám sát, bảo vệ an toàn thông tin; đơn vị độc lập kiểm tra, đánh giá định kỳ; thực hiện kết nối, chia sẻ, giám sát, cảnh báo an ninh mạng thường xuyên, liên tục theo hướng dẫn của cơ quan có thẩm quyền.

- Ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng "Made in Vietnam" đã qua kiểm định, đánh giá chất lượng theo quy định.

- Chủ động xây dựng kịch bản ứng phó đối với các tình huống tấn công mạng có thể xảy ra. Rà soát, hoàn thiện quy trình quản lý, lưu trữ, truyền đưa, xử lý tài liệu, dữ liệu thuộc phạm vi bí mật Nhà nước trên môi trường mạng; bảo đảm việc xử lý, trao đổi, lưu trữ, sao chụp, truyền đưa tài liệu, dữ liệu bí mật Nhà nước thực hiện đúng quy định pháp luật.

- Tăng cường quản lý, bảo vệ dữ liệu cá nhân, dữ liệu quan trọng, dữ liệu dùng chung, dữ liệu nhạy cảm; kiểm soát chặt chẽ việc thu thập, lưu trữ, khai thác, kết nối, chia sẻ dữ liệu theo quy định.

- Tăng cường kiểm tra việc quản lý, sử dụng thiết bị, phần mềm, nền tảng số, tài khoản cá nhân, dịch vụ lưu trữ, truyền nhận dữ liệu phục vụ xử lý thông tin, tài liệu công vụ, tài liệu mật; không sử dụng hệ thống, thiết bị, nền tảng không bảo đảm an toàn để xử lý thông tin, tài liệu theo quy định.

4. Đẩy mạnh tuyên truyền, nâng cao nhận thức, xây dựng văn hóa an toàn trên không gian mạng

- Đẩy mạnh tuyên truyền, phổ biến kiến thức pháp luật, kỹ năng cơ bản về an ninh mạng, an toàn thông tin, bảo mật thông tin, an ninh dữ liệu, bảo vệ dữ liệu cá nhân, phòng chống lừa đảo trực tuyến, phòng chống tin giả, thông tin xấu độc, bảo vệ trẻ em trên môi trường mạng.

- Tăng cường phát huy vai trò của Tổ công nghệ số cộng đồng và hệ thống thông tin cơ sở trong tuyên truyền, phổ biến kiến thức, hướng dẫn người dân sử dụng môi trường mạng an toàn; nâng cao kỹ năng số, kỹ năng bảo vệ dữ liệu cá nhân và phòng ngừa lừa đảo trên không gian mạng.

- Lồng ghép phổ biến kiến thức, kỹ năng an toàn, an ninh mạng trong hoạt động giáo dục, ngoại khóa, trải nghiệm, câu lạc bộ, cuộc thi tại các cơ sở giáo dục theo quy định và phù hợp với điều kiện thực tế.

- Phát triển văn hóa số bảo đảm giữ gìn bản sắc dân tộc, triển khai bộ quy tắc ứng xử trên không gian mạng, giảm thiểu tác động tiêu cực của công nghệ số đối với xã hội.

5. Xây dựng thế trận an ninh Nhân dân gắn với thế trận quốc phòng toàn dân trên không gian mạng

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, sức mạnh tổng hợp các tầng lớp Nhân dân trong bảo vệ an ninh mạng. Bảo đảm an toàn, an ninh mạng và chủ quyền quốc gia trên nền tảng số và không gian mạng; đảm bảo an ninh, an toàn dữ liệu hợp pháp của tổ chức, cá nhân, doanh nghiệp và chủ quyền an ninh dữ liệu quốc gia.

6. Nâng cao chất lượng nguồn nhân lực

- Rà soát, đánh giá thực trạng nhân lực tham gia công tác bảo đảm an ninh mạng, an toàn thông tin, quản trị, vận hành hệ thống thông tin tại các cơ quan, đơn vị thuộc phạm vi quản lý của xã.

- Kiện toàn đầu mối phụ trách công tác an toàn thông tin, an ninh mạng tại 100% cơ quan, đơn vị; xây dựng danh sách đầu mối để phục vụ đào tạo, tập huấn, cảnh báo, phối hợp xử lý sự cố.

- Cử cán bộ tham gia các khóa đào tạo, huấn luyện, diễn tập, sát hạch, cấp chứng nhận kiến thức, kỹ năng chuyên sâu về an ninh mạng theo hướng dẫn của Công an tỉnh, Sở Khoa học và Công nghệ, cơ quan có thẩm quyền.

- Tăng cường liên kết giữa Nhà nước - Nhà trường - Doanh nghiệp trong đào tạo, bồi dưỡng, huấn luyện thực hành, thực chiến định kỳ; nghiên cứu, đề xuất cơ chế thu hút, trọng dụng chuyên gia an ninh mạng chất lượng cao phù hợp thẩm quyền và điều kiện của xã.

7. Tăng cường hợp tác, liên kết trong lĩnh vực an ninh mạng

- Tăng cường liên kết giữa các cơ quan, đơn vị trong chia sẻ thông tin, cảnh báo sớm, phối hợp phòng, chống và ứng phó nguy cơ, sự cố tấn công mạng.

- Tham gia các hoạt động hợp tác, đào tạo, tập huấn, diễn tập, hội nghị, hội thảo, chia sẻ kinh nghiệm về an ninh mạng theo yêu cầu, hướng dẫn của cơ quan có thẩm quyền.

IV. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch được bố trí từ ngân sách Nhà nước theo phân cấp ngân sách hiện hành; lồng ghép trong các chương trình, đề án, dự án có liên quan và các nguồn kinh phí hợp pháp khác theo quy định.

V. TỔ CHỨC THỰC HIỆN

1. Công an xã

- Chủ trì, tham mưu UBND xã, Chủ tịch UBND xã tổ chức triển khai thực hiện Kế hoạch; hướng dẫn, theo dõi, đôn đốc, kiểm tra, tổng hợp kết quả thực hiện; chủ trì tham mưu sơ kết, tổng kết, báo cáo theo quy định.

- Chủ trì, tham mưu triển khai các nhiệm vụ về bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu; tăng cường công tác nắm tình hình, phòng ngừa, phát hiện, cảnh báo, xử lý nguy cơ mất an ninh mạng, lộ lọt dữ liệu, xâm phạm bí mật Nhà nước, dữ liệu cá nhân và dữ liệu quan trọng; phối hợp với các cơ quan, đơn vị liên quan trong phòng ngừa, phát hiện, xử lý các hành vi vi phạm pháp luật trên không gian mạng theo quy định.

- Chủ trì, phối hợp với Văn phòng HĐND và UBND, Phòng Văn hóa - Xã

hội, Ban Chỉ huy Quân sự xã và các cơ quan, đơn vị, tổ chức liên quan thực hiện giám sát, cảnh báo, ứng cứu, xử lý sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý của xã theo hướng dẫn của cơ quan có thẩm quyền.

- Chủ trì, theo dõi, hướng dẫn, phối hợp rà soát, phát hiện, cảnh báo và hỗ trợ xử lý nguy cơ mất an ninh mạng, nguy cơ lộ lọt dữ liệu, tài khoản, nguy cơ mất an toàn hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý của xã theo quy định.

- Tham mưu UBND xã cử cán bộ, công chức tham gia các cuộc diễn tập về an toàn thông tin, an ninh mạng do Công an tỉnh và cơ quan có thẩm quyền tổ chức.

- Tham mưu UBND xã hướng dẫn các cơ quan, đơn vị, tổ chức trực tiếp quản lý, vận hành hệ thống thông tin, cơ sở dữ liệu xây dựng hồ sơ, đề xuất và hoàn thiện phê duyệt cấp độ an toàn thông tin, an ninh mạng theo quy định.

- Chủ trì, nghiên cứu, rà soát, đề xuất giải pháp nâng cao năng lực giám sát, bảo đảm an ninh mạng phù hợp với hướng dẫn của Công an tỉnh và điều kiện thực tế của xã; trong đó nghiên cứu các giải pháp kỹ thuật, mô hình tổ chức phù hợp phục vụ giám sát, cảnh báo, điều phối ứng cứu sự cố an ninh mạng.

- Tăng cường công tác quản lý không gian mạng trên địa bàn xã, tập trung đấu tranh, xử lý dứt điểm tình trạng SIM "rác", tài khoản "ảo", thông tin xấu độc; bảo đảm trật tự, kỷ cương trong hoạt động của người dùng mạng xã hội; bảo đảm các yêu cầu về bảo vệ an ninh mạng quốc gia, bảo vệ dữ liệu cá nhân và bảo vệ trẻ em trên không gian mạng.

- Chủ trì, tổng hợp, báo cáo UBND xã, Chủ tịch UBND xã và Công an tỉnh theo quy định.

2. Ban Chỉ huy Quân sự xã

Bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo phạm vi quản lý, chức năng nhiệm vụ được giao. Phối hợp chặt chẽ với Công an xã trong công tác bảo đảm an ninh mạng chung.

3. Phòng Văn hóa - Xã hội

- Phối hợp với Công an xã theo dõi, hướng dẫn, phối hợp rà soát, phát hiện, cảnh báo và hỗ trợ xử lý nguy cơ mất an ninh mạng, nguy cơ lộ lọt dữ liệu, tài khoản, nguy cơ mất an toàn hệ thống thông tin, cơ sở dữ liệu thuộc phạm vi quản lý của xã theo quy định.

- Phối hợp tổ chức liên quan thực hiện giám sát, cảnh báo, ứng cứu, xử lý sự cố an ninh mạng đối với hệ thống thông tin thuộc phạm vi quản lý của xã theo hướng dẫn của cơ quan có thẩm quyền.

4. Phòng Kinh tế

Tham mưu UBND xã bố trí kinh phí đối với các nhiệm vụ chi của ngân sách cho hoạt động an ninh mạng, bảo mật thông tin, an ninh dữ liệu của xã.

5. Văn phòng HĐND và UBND

Phối hợp với Công an xã trong công tác bảo vệ an ninh mạng, bảo mật

thông tin và an ninh dữ liệu đối với các hệ thống thông tin trong phạm vi quản lý của xã. Tham mưu bố trí cán bộ phụ trách về an toàn thông tin, an ninh mạng của UBND xã.

6. Trung tâm Dịch vụ tổng hợp

Xây dựng nội dung tuyên truyền, phổ biến kiến thức pháp luật, kỹ năng cơ bản về an ninh mạng, an toàn thông tin, bảo mật thông tin, an ninh dữ liệu, bảo vệ dữ liệu cá nhân, phòng chống lừa đảo trực tuyến, phòng chống tin giả, thông tin xấu độc, bảo vệ trẻ em trên hệ thống truyền thanh thông minh, môi trường mạng trên các nền tảng số.

7. Các trường học thuộc UBND xã

Tổ chức các hoạt động giáo dục, ngoại khóa, trải nghiệm, câu lạc bộ, cuộc thi về kiến thức, kỹ năng an toàn, an ninh mạng cho các giáo viên, học sinh phù hợp theo quy định và phù hợp với điều kiện thực tế.

Thực hiện quản lý, vận hành hệ thống thông tin, xây dựng hồ sơ, đề xuất và hoàn thiện phê duyệt cấp độ an toàn thông tin, an ninh mạng theo quy định.

8. Trạm Y tế xã

Thực hiện quản lý, vận hành hệ thống thông tin, xây dựng hồ sơ, đề xuất và hoàn thiện phê duyệt cấp độ an toàn thông tin, an ninh mạng theo quy định.

9. Các cơ quan, đơn vị, tổ chức có liên quan

- Rà soát toàn bộ phần mềm, ứng dụng đang sử dụng để gỡ bỏ triệt để các sản phẩm không rõ nguồn gốc hoặc không có bản quyền; đồng thời cài đặt phần mềm diệt virus bản quyền và duy trì chế độ quét tự động thường xuyên. Ưu tiên sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng "Made in Vietnam" theo quy định.

- Tham gia đầy đủ các khóa học, chương trình về an toàn thông tin, an ninh mạng trên nền tảng "Bình dân học vụ số" của Bộ Công an (*sau khi có sử dụng sản phẩm, giải pháp, dịch vụ an ninh mạng "Made in Vietnam" theo quy định hướng dẫn của cơ quan có thẩm quyền*).

- Phối hợp với Công an xã, Văn phòng HĐND và UBND trong công tác bảo vệ an ninh mạng, bảo mật thông tin và an ninh dữ liệu đối với các hệ thống thông tin trong phạm vi quản lý của xã.

10. Các Tổ công nghệ số cộng đồng

Tích cực tuyên truyền, phổ biến kiến thức, hướng dẫn người dân sử dụng môi trường mạng an toàn; nâng cao kỹ năng số, kỹ năng bảo vệ dữ liệu cá nhân và phòng ngừa lừa đảo trên không gian mạng.

Trên đây là kế hoạch tổ chức thực hiện Chương trình hành động số 28-CTr/TU, ngày 24/6/2026 của Ban Thường vụ Tỉnh ủy An Giang về 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 trên địa bàn xã Vĩnh Thuận. Yêu cầu các cơ quan, đơn vị tổ chức nghiêm

túc triển khai thực hiện, trong quá trình triển khai, nếu có vướng mắc báo cáo UBND xã (qua Công an xã tổng hợp) để xem xét, giải quyết./.

Nơi nhận:
- PA05 – Công an tỉnh (b/c);
- Thường trực Đảng ủy xã (b/c);
- Thường trực HĐND xã;
- Chủ tịch và các PCT UBND xã;
- Các phòng, ban, ngành xã;
- Các trường thuộc UBND xã;
- Tổ Công nghệ số cộng đồng;
- Lưu: VT, CAX.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

U.B.N.D XÃ VĨNH THUẬN T. AN GIANG

Nguyễn Thanh Trung