ỦY BAN NHÂN DÂN XÃ ĐẠI ĐỒNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 106/KH-UBND	*Đại Đồng, ngày 29 tháng 5 năm 2026*

KẾ HOẠCH
Bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trên địa bàn xã Đại Đồng

Căn cứ Kế hoạch số 04-KH/BCĐTW ngày 05/01/2026 của Ban Chỉ đạo Trung ương về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số *(gọi tắt là Kế hoạch số 04-KH/BCĐTW)*; Chương trình hành động số 09-CTr/TU ngày 13/02/2026 của Tỉnh ủy thực hiện Chỉ thị số 57-CT/TW ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị (*Chương trình hành động số 09-CTr/TU)*;

Thực hiện Kế hoạch số 107/KH-UBND ngày 31/3/2026 của Ủy ban nhân dân tỉnh Hưng Yên về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị tỉnh Hưng Yên (*Kế hoạch số 107/KH-UBND*), Ủy ban nhân dân xã Đại Đồng ban hành Kế hoạch thực hiện trên địa bàn xã như sau:

I. MỤC ĐÍCH, YÊU CẦU

1. Mục đích

a) Quán triệt, phổ biến sâu rộng trong cán bộ, đảng viên, công chức, viên chức và các tầng lớp Nhân dân toàn xã, nhằm triển khai thực hiện nghiêm túc, kịp thời, hiệu quả các quan điểm chỉ đạo, mục tiêu, yêu cầu, nhiệm vụ trong Kế hoạch số 04-KH/BCĐTW; Chương trình hành động số 09-CTr/TU; Kế hoạch số 107/KH-UBND và các mục tiêu, nhiệm vụ, giải pháp, chỉ tiêu đã được giao trong các văn bản khác có liên quan.

b) Góp phần nâng cao nhận thức của cán bộ, đảng viên, công chức, viên chức và các tầng lớp Nhân dân toàn xã về bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu, từ đó nâng cao tinh thần tự giác, chủ động biệp pháp bảo vệ bản thân, bảo vệ dữ liệu, thông tin trên không gian mạng, phòng ngừa, đấu tranh những hành vi vi phạm pháp luật trên không gian mạng.

c) Đưa công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trở thành nhiệm vụ trọng yếu, thường xuyên của cả hệ thống chính trị; là nền tảng quan trọng bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng, bảo đảm an ninh chính trị, trật tự an toàn xã hội; tạo môi trường số an toàn, tin cậy phục vụ chuyển đổi số, phát triển chính quyền số, kinh tế số, xã hội số; chủ động phòng ngừa, ngăn chặn nguy cơ tụt hậu, bị động trước các thách thức an ninh phi truyền thống, góp phần xây dựng tỉnh phát triển nhanh, bền vững trong kỷ nguyên số.

2. Yêu cầu

a) Xác định rõ các nhiệm vụ cụ thể của từng phòng, ngành, đơn vị thuộc xã trong việc triển khai thực hiện Kế hoạch; bảo đảm phân công rõ trách nhiệm, rõ tiến độ, rõ kết quả đầu ra; thực hiện đồng bộ, thống nhất, hiệu quả các nhiệm vụ về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trong hệ thống chính trị trên địa bàn xã.

b) Gắn bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu với quá trình chuyển đổi số của xã; bảo đảm an toàn thông tin là điều kiện tiên quyết, xuyên suốt trong xây dựng chính quyền số, phát triển kinh tế số, xã hội số; không đánh đổi an toàn, an ninh mạng lấy tiến độ triển khai các ứng dụng, nền tảng số.

c) Phát huy tối đa các nguồn lực, triển khai đồng bộ các nhiệm vụ, giải pháp đã đề ra; thực hiện rà soát hằng năm và tổ chức sơ kết, tổng kết theo định kỳ 01 năm, 05 năm để đánh giá toàn diện kết quả thực hiện Kế hoạch; kịp thời điều chỉnh, bổ sung các nhiệm vụ, giải pháp phù hợp với tình hình thực tiễn, bảo đảm hoàn thành các mục tiêu đề ra.

d) Việc triển khai thực hiện Kế hoạch phải gắn với các chương trình, kế hoạch của UBND tỉnh đã ban hành liên quan đến hoạt động khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số trong tất cả các lĩnh vực, đồng thời phải đảm bảo phù hợp, thiết thực, hiệu quả tại địa phương.

II. MỤC TIÊU

1. Mục tiêu chung

a) Góp phần xây dựng không gian mạng quốc gia của tỉnh, của xã Đại Đồng bảo đảm an toàn, vững mạnh, có năng lực phòng vệ tốt và khả năng chống chịu cao, bảo vệ vững chắc chủ quyền, an ninh và lợi ích của quốc gia trên không gian mạng.

b) Nâng cao hiệu lực, hiệu quả của công tác bảo đảm đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu xã với sự chung tay vào cuộc triển khai thực hiện các nhiệm vụ an toàn, an ninh mạng của cả hệ thống chính trị.

2. Mục tiêu cụ thể năm 2026

a) Về tổ chức, nhận thức

- Tạo chuyển biến mạnh mẽ về nhận thức và trách nhiệm của các cấp ủy, chính quyền, cơ quan, đơn vị và đội ngũ cán bộ, đảng viên đối với công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu; xác định đây là nhiệm vụ trọng yếu, thường xuyên của toàn hệ thống chính trị.

- 100% lãnh đạo phòng, ngành, đơn vị thuộc xã cán bộ chuyên trách công nghệ thông tin được tập huấn, bồi dưỡng nâng cao nhận thức về an ninh mạng, bảo mật thông tin và an ninh dữ liệu.

b) Về an ninh mạng

- Căn cứ hướng dẫn của cấp trên, chủ động rà soát, xây dựng, ban hành Quyết định về quy chế bảo đảm an ninh mạng của xã; rà soát, xây dựng Hồ sơ

đề xuất cấp độ an toàn an ninh mang, trình, đề nghị cơ quan có thẩm quyền phê duyệt, nhằm triển khai thực hiện đồng bộ các giải pháp đảm bảo an toàn an ninh mạng, thông tin mạng và an ninh dữ liệu.

- Rà soát hạ tầng CNTT hiện có, xem xét, đầu tư, nâng cấp hạ tầng công nghệ, đảm bảo cơ bản đáp ứng yêu cầu và phục vụ phát triển kinh tế số, xã hội số, xây dựng chính quyền số trong kỷ nguyên số.

- Phối hợp với các phòng chuyên môn Công an tỉnh phối hợp triển khai thực hiện các giải pháp nhằm nâng cao hiệu quả công tác giám sát và ứng cứu sự cố an ninh mạng, đảm bảo 100% hệ thống thông tin quan trọng của các cơ quan Đảng, Nhà nước trên địa bàn xã được triển khai mô hình bảo vệ và được giám sát an toàn thông tin 24/7.

c) Về bảo mật thông tin

- Xây dựng, ban hành, tổ chức thực hiện Quy chế bảo đảm an toàn thông tin, bảo mật thông tin và bảo vệ bí mật nhà nước trên môi trường mạng; 100% các phòng, ngành, đơn vị thuộc xã triển khai thực hiện nghiêm Quy chế bảo đảm an toàn thông tin, bảo mật thông tin và bảo vệ bí mật nhà nước trên môi trường mạng.

- 100% hệ thống xử lý thông tin bí mật nhà nước được áp dụng giải pháp mật mã, ký số, mã hóa theo quy định; thực hiện kiểm soát truy cập, phân quyền và lưu vết truy cập theo quy định.

d) Về an ninh dữ liệu

- Phối hợp triển khai thực hiện rà soát, phân loại dữ liệu dùng chung, dữ liệu chuyên ngành theo tính chất quan trọng của dữ liệu và các quy định về bảo vệ dữ liệu cá nhân, bảo vệ bí mật nhà nước.

- 100% dữ liệu quan trọng được thực hiện sao lưu định kỳ và có phương án phục hồi khi xảy ra sự cố; bảo đảm nguyên tắc "an toàn ngay từ thiết kế" đối với các dự án công nghệ thông tin, chuyển đổi số mới.

3. Mục tiêu đến năm 2030

a) Về an ninh mạng

- Thụ hưởng, vận hành hiệu quả Kiến trúc bảo vệ an ninh mạng xã theo mô hình phòng thủ đa lớp, hiện đại, đồng bộ, phù hợp với Kiến trúc bảo vệ an ninh mạng quốc gia; bảo đảm 100% hệ thống thông tin của các cơ quan Đảng, Nhà nước trên địa bàn xã được bảo vệ và được giám sát an toàn thông tin 24/7.

- Kết nối, phối hợp triển khai thực hiện theo Trung tâm giám sát và điều hành an ninh mạng tỉnh, đảm bảo ổn định, hiệu quả; kết nối, chia sẻ thông tin an ninh mạng đối với toàn bộ hệ thống thông tin quan trọng, cơ sở dữ liệu dùng chung và chuyên ngành trên địa bàn.

- 100% phòng, ban, ngành, đơn vị thuộc xã triển khai đánh giá rủi ro an ninh mạng định kỳ hằng năm và áp dụng hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia.

b) Về bảo mật thông tin: Cơ quan UBND xã duy trì 100% thực hiện nghiêm quy chế bảo mật thông tin, bảo vệ bí mật nhà nước trên môi trường

mạng; không để xảy ra lộ, lọt bí mật nhà nước do nguyên nhân chủ quan. 100% hệ thống thông tin quan trọng áp dụng cơ chế xác thực đa yếu tố, phân quyền truy cập chặt chẽ, giám sát và kiểm soát truy cập bất thường; 100% các phòng, ban, ngành, đơn vị thuộc xã nghiêm chỉnh thực hiện quy chế bảo mật thông tin, bảo vệ bí mật nhà nước trên môi trường mạng; không để xảy ra lộ, lọt bí mật nhà nước do nguyên nhân chủ quan.

c) Về an ninh dữ liệu

- Hoàn thành kết nối, chia sẻ liệu dùng chung, dữ liệu chuyên ngành của xã với Cổng dịch vụ công Quốc gia, kết nối với hệ thống thủ tục của các bộ, ngành và kết nối, chia sẻ với Trung tâm dữ liệu tỉnh đạt chuẩn an ninh mạng.

- 100% dữ liệu quan trọng được mã hóa khi lưu trữ và truyền dẫn; được sao lưu, dự phòng và kiểm tra khả năng phục hồi định kỳ.

- Triển khai mô hình quản trị dữ liệu tập trung, bảo đảm dữ liệu được quản lý, khai thác, chia sẻ an toàn trong toàn bộ vòng đời, góp phần bảo đảm chủ quyền dữ liệu số của tỉnh.

d) Về nhận thức, nhân lực an ninh mạng

- 100% lãnh đạo các phòng, ban, ngành, đơn vị thuộc xã được bồi dưỡng, cập nhật kiến thức về an ninh mạng và bảo vệ dữ liệu trong quá trình lãnh đạo, chỉ đạo chuyển đổi số.

- 100% cán bộ chuyên trách, phụ trách công nghệ thông tin tại các cơ quan nhà nước trên địa bàn xã được đào tạo, bồi dưỡng chuyên sâu về an toàn thông tin, an ninh mạng, đủ năng lực quản trị, vận hành và bảo vệ hệ thống thông tin. 100% cán bộ, công chức làm việc với dữ liệu quan trọng, dữ liệu cá nhân được tập huấn kỹ năng nhận diện và phòng chống tấn công bằng công nghệ AI (Deepfake, mã độc thế hệ mới...).

- Phối hợp với đội ngũ chuyên gia an ninh mạng của tỉnh có năng lực làm chủ công nghệ, nhằm tham gia vận hành hệ thống giám sát an ninh mạng và kịp thời xử lý các sự cố an ninh mạng.

- Nhận thức và kỹ năng cơ bản về an toàn thông tin, bảo vệ dữ liệu cá nhân được phổ biến rộng rãi trong xã hội; người dân và doanh nghiệp từng bước nâng cao khả năng phòng tránh các nguy cơ mất an toàn thông tin trên môi trường mạng.

III. NHIỆM VỤ, GIẢI PHÁP

1. Tăng cường sự lãnh đạo, chỉ đạo; nâng cao nhận thức và trách nhiệm

a) Quán triệt, triển khai thực hiện nghiêm các chủ trương của Đảng, Nhà nước về bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; xác định đây là nhiệm vụ trọng yếu, thường xuyên của toàn hệ thống chính trị trên địa bàn tỉnh.

b) Gắn trách nhiệm người đứng đầu cơ quan, đơn vị với kết quả công tác bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu; coi đây là tiêu chí đánh giá, xếp loại hằng năm.

c) Tham gia đầy đủ các chương trình đạo tạo, bồi dưỡng, tập huấn, nhằm nâng cao nhận thức cho 100% lãnh đạo phòng, ban, ngành, đơn vị thuộc xã và cán bộ chuyên trách công nghệ thông tin về an ninh mạng, bảo mật thông tin, an ninh dữ liệu và trách nhiệm bảo đảm an toàn hệ thống theo cấp độ.

d) Đẩy mạnh tuyên truyền, phổ biến kiến thức, kỹ năng an toàn thông tin cho cán bộ, đảng viên, công chức, viên chức và Nhân dân; phát động phong trào toàn dân tham gia bảo vệ an ninh mạng.

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

a) Chủ động rà soát, tham mưu cấp có thẩm quyền tiến hành sửa đổi, bổ sung hoặc thay thế các quy chế, quy định về quy chế bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu; quản lý, vận hành, khai thác hệ thống thông tin, cơ sở dữ liệu; quy chế bảo vệ bí mật nhà nước trên không gian mạng hiệu quả theo quy định.

b) Thực hiện nghiêm quy định về xác định và phê duyệt cấp độ an toàn hệ thống thông tin; bảo đảm 100% hệ thống thông tin của xã được triển khai phương án bảo đảm an toàn theo cấp độ đã được phê duyệt.

c) Việc đề xuất xây dựng các dự án ứng dụng công nghệ thông tin, chuyển đổi số phải có cấu phần an ninh mạng, bảo mật thông tin, an ninh dữ liệu được thẩm định trước khi triển khai thực hiện.

d) Áp dụng thực hiện hiệu quả Khung quản trị rủi ro an ninh mạng quốc gia; thực hiện quản trị hệ thống dựa trên đánh giá rủi ro, tiêu chuẩn, quy chuẩn kỹ thuật.

đ) Chủ động phối hợp, chia sẻ thông tin, báo cáo sự cố an ninh mạng với Công an tỉnh và các sở, ngành, cơ quan, đơn vị liên quan, nhằm kịp thời ứng cứu sự cố, tránh những rủi ro, mất an toàn thông tin, an ninh mạng.

3. Bảo đảm an ninh mạng đối với hệ thống thông tin

a) Triển khai đầy đủ mô hình bảo theo yêu cầu của cấp có thẩm quyền; bảo đảm 100% hệ thống thông tin của các cơ quan Đảng, Nhà nước trên địa bàn tỉnh được giám sát an toàn thông tin 24/7.

b) Phối hợp, kết nối với Hệ thống Trung tâm giám sát và điều hành an ninh mạng tỉnh, nhằm bảo đảm theo dõi sát sao hệ thống, kịp thời phản ánh, xử lý khi có phát sinh sự cố.

c) Thực hiện theo yêu cầu, chỉ đạo của Công an tỉnh về đánh giá, khắc phục lỗ hổng, điểm yếu an ninh mạng; rà soát, kiểm tra an ninh đối với các thiết bị phần cứng, phần mềm và dịch vụ CNTT do các đối tác bên thứ ba cung cấp, đặc biệt là các thiết bị có nguồn gốc từ nước ngoài hoặc sử dụng công nghệ mã nguồn đóng; định kỳ tham gia công tác diễn tập, ứng cứu sự cố an ninh mạng.

d) Ưu tiên sử dụng sản phẩm, giải pháp an ninh mạng "Make in Viet Nam"; ứng dụng trí tuệ nhân tạo, phân tích dữ liệu lớn và công nghệ tiên tiến trong giám sát, cảnh báo sớm và phòng thủ chủ động.

4. Tăng cường bảo mật thông tin và bảo vệ bí mật nhà nước trên không gian mạng

a) Rà soát, phân loại thông tin theo mức độ "Công khai, Nội bộ, Hạn chế, Bí mật nhà nước"; quản lý chặt chẽ việc soạn thảo, lưu trữ, truyền đưa, khai thác thông tin mật trên môi trường mạng.

b) Triển khai sử dụng đồng bộ giải pháp mật mã, chữ ký số, mã hóa dữ liệu trong trao đổi văn bản điện tử, xử lý công việc và lưu trữ thông tin bí mật nhà nước theo quy định.

c) Kiểm soát chặt chẽ quyền truy cập hệ thống; thực hiện phân quyền, xác thực đa yếu tố, ghi nhật ký và giám sát truy cập đối với các hệ thống xử lý thông tin quan trọng.

d) Phối hợp chặt chẽ với thanh tra chuyên ngành, nhằm kịp thời phát hiện những sai phạm, lỗ hổng bảo mật, qua đó xử lý (đề nghị xử lý) nghiêm các hành vi vi phạm quy định về bảo mật thông tin, để lộ, lọt bí mật nhà nước.

5. Bảo đảm an ninh dữ liệu và chủ quyền dữ liệu số của xã

a) Hoàn thành kết nối, vận hành, khai thác dữ liệu dùng chung và dữ liệu chuyên ngành với Bộ, ngành, cấp tỉnh tại Trung tâm dữ liệu tỉnh đạt chuẩn an ninh mạng; chấm dứt tình trạng lưu trữ phân tán, máy chủ không bảo đảm an toàn tại cấp cơ sở.

b) Ban hành và thực hiện quy chế quản lý, khai thác, chia sẻ và bảo vệ dữ liệu; xác định rõ trách nhiệm của cơ quan chủ quản dữ liệu và đơn vị vận hành hệ thống.

c) Thực hiện sao lưu, dự phòng và phục hồi dữ liệu định kỳ; bảo đảm 100% dữ liệu quan trọng có phương án khôi phục khi xảy ra sự cố, tấn công mạng theo hướng dẫn của cấp trên.

d) Bảo đảm nguyên tắc "an toàn ngay từ thiết kế" trong xây dựng cơ sở dữ liệu, nền tảng số; dữ liệu được bảo vệ trong toàn bộ vòng đời từ thu thập, xử lý, lưu trữ, chia sẻ đến hủy bỏ.

đ) Bảo đảm tính toàn vẹn, sẵn sàng và bí mật của dữ liệu trong mọi tình huống, nhất là tăng cường bảo đảm an ninh luồng dữ liệu kết nối liên thông.

6. Phát triển nguồn nhân lực an ninh mạng

a) Thường xuyên kiện toàn đội ngũ chuyên trách an ninh mạng của xã. 100% cán bộ chuyên trách công nghệ thông tin được đào tạo, bồi dưỡng chuyên sâu về an ninh mạng.

b) Tăng cường liên kết giữa cơ quan nhà nước, cơ sở đào tạo và doanh nghiệp trong đào tạo, huấn luyện thực hành, góp phần xây dựng mạng lưới chuyên gia hỗ trợ ứng cứu sự cố.

7. Bảo đảm nguồn lực tài chính, ngân sách

a) Bố trí kinh phí bảo đảm cho công tác an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo phân cấp ngân sách; ưu tiên đầu tư có trọng tâm, trọng điểm, tránh dàn trải. 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 và chuyển đổi số; đầu tư có trọng tâm, trọng điểm, tránh dàn trải, lãng phí.

b) Ưu tiên sử dụng sản phẩm, dịch vụ an ninh mạng, an toàn thông tin "Make in Vietnam" đáp ứng yêu cầu bảo đảm an ninh mạng, bảo mật dữ liệu và an toàn thông tin bảo vệ an ninh mạng cho các cơ quan nhà nước trên địa bàn.

8. Danh mục các nhiệm vụ giao các phòng, ban, ngành, đơn vị thực hiện

(Chi tiết tại Phụ lục kèm theo).

IV. TỔ CHỨC THỰC HIỆN

1. Các phòng, ban, ngành, đơn vị liên quan: Chủ động phối hợp xây dựng Kế hoạch, phương án, giải pháp về đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong cơ quan, đơn vị theo chức năng, nhiệm vụ; định kỳ báo cáo kết quả thực hiện về UBND xã để tổng hợp, báo cáo UBND tỉnh, Công an tỉnh theo quy định. Thường xuyên rà soát, cập nhật, bổ sung các nhiệm vụ vào kế hoạch, chương trình công tác hằng năm của cơ quan, đơn vị để tổ chức triển khai thực hiện. Kết quả thực hiện công tác bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu là một trong các tiêu chí đánh giá mức độ hoàn thành nhiệm vụ, bình xét thi đua, khen thưởng hằng năm của người đứng đầu cơ quan, đơn vị.

2. Thủ trưởng các phòng, ban, ngành, đơn vị thuộc xã: Chủ động chỉ đạo, triển khai thực hiện các nội dung nhiệm vụ, giải pháp cụ thể được giao tại Kế hoạch và Phụ lục kèm theo; tăng cường theo dõi, đôn đốc, kiểm tra việc triển khai thực hiện; định kỳ 6 tháng ***(trước ngày 10/6)*** và hằng năm ***(trước ngày 10/11)*** báo cáo UBND xã *(qua Văn phòng HĐND&UBND xã)* để tổng hợp, báo cáo theo quy định.

3. Phòng Kinh tế: Chủ trì, phối hợp với các phòng, ngành, đơn vị liên quan tham mưu UBND xã bố trí kinh phí từ ngân sách địa phương để triển khai các nhiệm vụ, giải pháp về bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu theo quy định; hàng năm hướng dẫn các cơ quan, đơn vị, địa phương lập dự toán, quản lý, sử dụng và quyết toán kinh phí thực hiện các nhiệm vụ bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu theo đúng quy định của pháp luật về ngân sách nhà nước. Phối hợp với các cơ quan, đơn vị liên quan tham mưu huy động, lồng ghép các nguồn lực hợp pháp khác để phục vụ triển khai các nhiệm vụ bảo đảm an ninh mạng, an toàn thông tin và an ninh dữ liệu trên địa bàn tỉnh.

4. Phòng Văn hóa - Xã hội xã: Chủ động phối hợp với Văn phòng HĐND&UBND xã trong triển khai thực hiện các nhiệm vụ đảm bảo an toàn thông tin, an ninh mạng, nhất là Quy chế bảo đảm an toàn hệ thống thông tin và an ninh mạng xã và Hồ sơ đề xuất cấp độ an toàn hệ thống thông tin, an ninh mạng xã theo chuẩn cấp độ 2, góp phần thúc đẩy phát triển kinh tế số, xã hội số, xây dựng chính quyền số

5. Giao Văn phòng HĐND&UBND xã: Chủ trì triển khai thực hiện các nhiệm vụ bảo đảm an toàn thông tin, an ninh mạng theo Kế hoạch, đảm thời tiến độ và thời gian theo quy định; phối hợp Phòng Văn hóa - Xã hội và các phòng,

ngành, đơn vị theo dõi, đôn đốc việc triển khai thực hiện Kế hoạch, kịp thời báo cáo và kiến nghị UBND tỉnh các biện pháp cần thiết để bảo đảm thực hiện đồng bộ và có hiệu quả Kế hoạch đồng thời tập hợp báo cáo theo quy định.

Trên đây là Kế hoạch bảo đảm an ninh mạng, bảo mật thông tin và an ninh dữ liệu trên địa bàn xã, Ủy ban nhân dân xã yêu cầu các phòng, ngành, đơn vị thuộc xã nghiêm túc triển khai thực hiện. Trong quá trình triển khai, thực hiện, nếu có khó khăn, vướng mắc, kịp thời phản ánh về UBND xã (Qua Văn phòng HĐND&UBND) để tổng hợp, báo cáo, xin ý kiến hướng dẫn giải quyết theo thẩm quyền hoặc trình cấp có thẩm quyền xem xét, quyết định./.

Nơi nhận:
- Ủy ban nhân dân tỉnh;
- Công an tỉnh;
- Sở Khoa học và Công nghệ tỉnh;
- Thường trực Đảng ủy - HĐND xã;
- Chủ tịch, các PCT UBND xã;
- Các phòng, ban, ngành, đơn vị xã;
- Cổng thông tin điện tử xã;
- Lưu: VT.

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

Trần Văn Thành