ỦY BAN NHÂN DÂN XÃ TÂN HỘI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 182/KH-UBND	*Tân Hội, ngày 04 tháng 8 năm 2026*

KẾ HOẠCH
Triển khai mô hình bảo đảm an toàn thông tin 4 lớp

Căn cứ Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

Căn cứ Kế hoạch số 18-KH/BCĐ ngày 24/6/2026 của Ban Chỉ đạo tỉnh về phát triển khoa học, công nghệ, đổi mới sáng tạo và chuyển đổi số tỉnh An Giang;

Căn cứ Công văn số 4136/CAT-ANM ngày 28/7/2026 của Công an tỉnh An Giang về triển khai mô hình bảo đảm an toàn thông tin 4 lớp.

Ủy ban nhân dân xã (UBND) ban hành Kế hoạch triển khai mô hình bảo đảm an toàn thông tin 4 lớp trên địa bàn xã Tân Hội, cụ thể như sau:

I. MỤC TIÊU, YÊU CẦU

1. Mục tiêu chung

Bảo đảm an toàn thông tin (viết tắt là ATTT) quan trọng trên địa bàn xã; bảo đảm khả năng thích ứng một cách chủ động, linh hoạt và giảm thiểu các nguy cơ đe dọa mất ATTT trên mạng, đề ra các giải pháp ứng phó khi gặp sự cố mất ATTT mạng. Xây dựng không gian mạng của xã an toàn, vững mạnh, có năng lực phòng vệ tốt, khả năng chống chịu cao, bảo vệ vững chắc chủ quyền, an ninh, lợi ích quốc gia, thông tin trên không gian mạng, ổn định chính trị, xã hội. 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 xã Tân Hội thuộc nhóm an toàn, an ninh không gian mạng, an ninh dữ liệu và bảo vệ dữ liệu.

2. Mục tiêu cụ thể

- Tạo chuyển biến mạnh mẽ về nhận thức và hành động trong toàn hệ thống chính trị và xã hội trên địa bàn xã.

- Rà soát, khắc phục 100% các lỗ hổng, điểm yếu an ninh mạng tại các hệ thống thông tin của cơ quan Đảng, Nhà nước, Mặt trận Tổ quốc và các đoàn thể.

- Đề xuất tỉnh phê duyệt cấp độ an toàn thông tin và triển khai mô hình "4 lớp" cho toàn bộ hệ thống chính trị.

- Nâng cao nhận thức của cán bộ, đảng viên và người dân về bảo mật thông tin, an ninh mạng và an ninh dữ liệu; giới thiệu cán bộ tham gia đào tạo, bồi dưỡng, tập huấn nội dung an ninh mạng chất lượng cao.

- Tăng cường kỷ luật, kỷ cương trong quản lý nhà nước về an ninh mạng; thực hiện quản trị an ninh mạng dựa trên đánh giá rủi ro, tuân thủ tiêu chuẩn, quy chuẩn kỹ thuật.

- Thúc đẩy ứng dụng các công nghệ tiên tiến như trí tuệ nhân tạo, phân tích dữ liệu lớn, giám sát thông minh để phát hiện sớm và xử lý kịp thời các mối đe dọa mạng. Chuyển đổi sang mô hình phòng thủ chủ động, các giải pháp mã hoá hiện đại phục vụ bảo vệ dữ liệu quan trọng, dữ liệu bí mật và giao dịch của Nhà nước.

3. Yêu cầu

Các hệ thống thông tin của các cơ quan trên địa bàn phải được đánh giá hiện trạng và khả năng bảo đảm an ninh mạng, dự báo các nguy cơ, sự cố để đưa ra phương án ứng phó, ứng cứu sự cố kịp thời, phù hợp.

- Hoạt động ứng cứu sự cố mất an toàn thông tin mạng phải chuyển từ bị động sang chủ động, bao gồm: Chủ động thực hiện săn lùng các mối nguy hại và rà soát lỗ hổng trên các hệ thống thông tin trong phạm vi quản lý.

- Thường xuyên trao đổi thông tin, chia sẻ kinh nghiệm trong công tác bảo đảm ATTT giữa các cơ quan trên địa bàn; tận dụng sự phối hợp, hỗ trợ của Công an tỉnh (Phòng an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao).

II. NỘI DUNG MÔ HÌNH

1. Lớp 1: Lực lượng tại chỗ (100% Cán bộ, công chức, viên chức và người lao động thuộc xã Tân Hội thực hiện)

Bố trí tối thiểu 01 cán bộ có trình độ chuyên môn hoặc có năng lực, kỹ năng về công nghệ thông tin làm đầu mối An ninh mạng.

- Đối với quản lý, kiểm soát hoạt động máy tính: Tuyệt đối không cài đặt các phần mềm lạ, trò chơi, hoặc phần mềm hỗ trợ từ xa khi không có yêu cầu kỹ thuật.

- Đối với kết nối mạng: Không sử dụng chung đường truyền Internet của cơ quan cho mục đích phát Wifi công cộng cho người lạ sử dụng.

2. Lớp 2: Giám sát bảo vệ chuyên nghiệp

- Triển khai bảo vệ điểm cuối: Đảm bảo các máy tính làm việc của các đơn vị phải được cấu hình, cài đặt phần mềm phòng chống mã độc và không được tự ý tắt, gỡ bỏ phần mềm này (bao gồm cả phần mềm mua bản quyền; phần mềm Windows Security).

- Luôn đảm bảo an toàn các tài khoản: Thực hiện đăng xuất toàn bộ tài khoản phần mềm dùng chung (Quản lý văn bản, Dịch vụ công...) sau khi không sử dụng, kết thúc buổi làm việc. Tuyệt đối không lưu mật khẩu trên trình duyệt web.

3. Lớp 3: Kiểm tra, đánh giá an ninh mạng độc lập

- Định kỳ tối thiểu 01 năm một lần thực hiện kiểm tra, đánh giá, rà quét, phát hiện lỗ hổng, điểm yếu, kiểm thử xâm nhập hệ thống.

- Hằng quý, cán bộ đầu mối thực hiện rà soát danh sách các máy tính trong mạng LAN; kiểm tra, hướng dẫn việc tuân thủ các quy định về bảo mật thông tin, trong đó

có việc thiết lập, đổi mật khẩu truy cập; thu hồi quyền truy cập của các cán bộ, công chức, viên chức đã chuyển công tác hoặc nghỉ việc.

- Chủ động rà quét mã độc toàn bộ hệ thống máy tính 06 tháng/lần. Kịp thời trao đổi, cung cấp thông tin, phối hợp khắc phục các sự cố xảy ra hoặc được điều phối từ cơ quan chuyên trách về an ninh mạng của tỉnh (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Công an tỉnh).

4. Lớp 4: Kết nối, chia sẻ với hệ thống giám sát mạng quốc gia

- Cử cán bộ làm đầu mối An ninh mạng tham gia đầy đủ các cuộc diễn tập ứng cứu sự cố an toàn thông tin do Công an tỉnh hoặc cơ quan có thẩm quyền tổ chức.

- Tổ chức diễn tập nội bộ tại đơn vị đối với các tình huống giả định về mã độc, tấn công mạng hoặc mất dữ liệu.

- Khi thấy máy tính có dấu hiệu bị chậm bất thường, file bị đổi đuôi (dấu hiệu mã hóa), hoặc mất quyền truy cập tài khoản, phải ngắt kết nối mạng ngay lập tức và báo cáo về Cán bộ đầu mối An ninh mạng, kịp thời báo cáo về Công an tỉnh (Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao) trong vòng 15 phút.

III. KINH PHÍ THỰC HIỆN

Kinh phí thực hiện Kế hoạch này được sử dụng từ nguồn ngân sách nhà nước theo phân cấp ngân sách hiện hành; lồng ghép với kinh phí thực hiện các chương trình, kế hoạch, đề án khác có liên quan và các nguồn kinh phí khác theo quy định của pháp luật.

IV. TỔ CHỨC THỰC HIỆN

1. Văn phòng HĐND-UBND xã

- Là cơ quan đầu mối, chuyên trách về ứng cứu sự cố ATTT mạng trên địa bàn xã, có trách nhiệm chủ trì theo dõi, đôn đốc, phối hợp với các cơ quan đơn vị tổ chức triển khai thực hiện Kế hoạch này.

- Tham mưu, tổ chức thực thi, đôn đốc, kiểm tra, đánh giá, giám sát, hướng dẫn công tác bảo đảm ATTT định kỳ hằng năm hoặc theo chỉ đạo của UBND tỉnh đối với các cơ quan nhà nước, doanh nghiệp trên địa bàn xã. Tiến hành xử lý theo quy định của pháp luật các cá nhân, cơ quan vi phạm trong công tác bảo đảm ATTT mạng.

- Phối hợp Phòng Văn hóa - Xã hội, Công an xã xây dựng hồ sơ đề xuất cấp độ an toàn hệ thống thông tin.

- Tham mưu cho UBND xã cử cán bộ có trình độ, kinh nghiệm tham gia xử lý, ứng cứu các sự cố về An ninh mạng, ATTT xảy ra trên địa bàn xã khi có yêu cầu.

2. Công an xã:

- Chủ trì, phối hợp với Văn phòng HĐND - UBND xã, các phòng, ban, ngành xã tổ chức diễn tập nội bộ tại UBND xã đối với các tình huống giả định về mã độc, tấn công mạng hoặc mất dữ liệu.

- Chủ trì, phối hợp Văn phòng HĐND - UBND xã và các phòng, ban, ngành liên quan đề xuất khen thưởng các tập thể, cá nhân có thành tích xuất sắc trong thực hiện Kế hoạch, nội dung diễn tập.

- Tổng hợp báo cáo, tham mưu Ủy ban nhân dân xã tổ chức hội nghị sơ kết hàng tháng *(xét thấy cần thiết)* và hội nghị tổng kết hàng năm.

Trên đây là kế hoạch triển khai mô hình bảo đảm an toàn thông tin 4 lớp. Yêu cầu các phòng, ban, ngành đoàn thể; cán bộ, công chức và cơ quan, tổ chức trên địa bàn triển khai thực hiện nghiêm túc; quá trình thực hiện có khó khăn, vướng mắc báo cáo UBND xã (qua Văn phòng HĐND-UBND) để tổng hợp trình lãnh đạo UBND xã giải quyết./.

Nơi nhận:
- Sở Khoa học và công nghệ;
- Công an tỉnh;
- Thường trực Đảng ủy xã;
- Thường Trực HĐND-UBND xã;
- UBMTTQ Việt Nam xã;
- Chủ tịch và các Phó Chủ tịch xã;
- Các phòng, ban, ngành xã;
- Trưởng các ấp trên địa bàn xã;
- Lưu: VT, PVHXH.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

Lê Quang Nhựt