ỦY BAN NHÂN DÂN XÃ PHẠM NGŨ LÃO	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập – Tự do – Hạnh phúc
Số: 491 /BC-UBND	*Xã Phạm Ngũ Lão, ngày 26 tháng 10 năm 2026*

BÁO CÁO
Kết quả triển khai phương án bảo đảm an toàn thông tin theo cấp độ đối với Hệ thống thông tin Mạng nội bộ (LAN) UBND xã Phạm Ngũ Lão

Thực hiện Công văn số 8462/CAT-ANM ngày 21/10/2026 của Công an tỉnh Hưng Yên về việc báo cáo kết quả triển khai phương án bảo đảm an toàn thông tin theo cấp độ;

Ủy ban nhân dân xã Phạm Ngũ Lão báo cáo kết quả triển khai phương án bảo đảm an toàn thông tin theo cấp độ đối với Hệ thống thông tin Mạng nội bộ (LAN) tại UBND xã, cụ thể như sau:

I. THÔNG TIN CHUNG VỀ HỆ THỐNG THÔNG TIN

Ủy ban nhân dân xã Phạm Ngũ Lão hiện quản lý 01 hệ thống thông tin đã được phê duyệt cấp độ, cụ thể như sau:

- Tên hệ thống: Hệ thống thông tin Mạng nội bộ (LAN) Ủy ban nhân dân xã Phạm Ngũ Lão.

- Đơn vị chủ quản: Ủy ban nhân dân tỉnh Hưng Yên.

- Đơn vị vận hành: Văn phòng HĐND-UBND xã trực tiếp vận hành hệ thống thông tin. Việc bảo đảm an toàn thông tin đối với phần hạ tầng, phần mềm, dữ liệu của các hệ thống này thuộc trách nhiệm của đơn vị chủ quản; UBND xã chịu trách nhiệm quản lý tài khoản người dùng và bảo đảm an toàn thông tin đối với máy trạm, thiết bị đầu cuối truy cập hệ thống

- Cấp độ an toàn thông tin: Cấp độ 2.

- Quyết định phê duyệt: Quyết định số 4311/QĐ-CAT-PA05 ngày 08/6/2026 của Công an tỉnh Hưng Yên về việc phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống thông tin Mạng nội bộ (LAN) Ủy ban nhân dân xã Phạm Ngũ Lão.

*** Khái quát hiện trạng hệ thống**

- Phạm vi, quy mô của hệ thống mạng nội bộ (Lan): Hệ thống được thiết lập để phục vụ công tác chỉ đạo, điều hành, trao đổi thông tin, khai thác các hệ thống dùng chung của tỉnh, đồng thời cung cấp kết nối mạng phục vụ người dân, doanh nghiệp thực hiện các thủ tục hành chính công tại Bộ phận Tiếp nhận và Trả kết quả của UBND xã Phạm Ngũ Lão.

- Các thành phần chính: Hệ thống được mạng nội bộ được đơn vị VNPT triển khai các thiết bị chung với các xã.

- Hạ tầng kỹ thuật, phần mềm: 02 Thiết bị tường lửa Fortinet FortiGate 60F; bộ chuyển mạch Switch C9200L-24T-4G-E Cisco Catalyst 9200L 24-port

Data 4x1G uplink Switch + Stackit + cab stack tại vùng mạng nội bộ; thiết bị cấp nguồn Switch Cisco 24 port Cisco C1300-24T-4G và 14 thiết bị phát WiFi UniFi tại vùng mạng WiFi; máy trạm của cán bộ, công chức phục vụ gửi, nhận văn bản, khai thác phần mềm nội bộ và in ấn tài liệu.

- Dữ liệu: UBND xã không có máy chủ riêng; các phần mềm dùng chung (Hệ thống quản lý văn bản, dịch vụ công và các phần mềm chuyên ngành) do tỉnh, Trung ương triển khai, dữ liệu lưu trữ tại hạ tầng của cơ quan quản lý hệ thống dùng chung. Dữ liệu cục bộ gồm tài liệu làm việc trên máy trạm, tập tin cấu hình thiết bị mạng.

- Hệ thống được khai thác thường xuyên, vận hành ổn định, phục vụ công tác chỉ đạo, điều hành và giải quyết thủ tục hành chính của UBND xã.

II. KẾT QUẢ TRIỂN KHAI CÁC BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN

1. Công tác quản lý và tổ chức thực hiện

- Quy chế, quy định: UBND xã đã ban hành Quyết định số 1096/QĐ-UBND ngày 29/5/2026 về việc ban hành Quy chế bảo đảm an toàn hệ thống thông tin, an ninh mạng hệ thống mạng nội bộ của UBND xã Phạm Ngũ Lão kèm theo

- Phân công trách nhiệm: UBND xã Phạm Ngũ Lão giao Công an xã là đầu mối liên hệ, phối hợp các cơ quan tổ chức có thẩm quyền quản lý về an toàn thông tin phục vụ việc bảo đảm an toàn, an ninh mạng cho Hệ thống mạng nội bộ. Bộ phận chuyên trách về an toàn thông tin có trách nhiệm tham gia đầy đủ các hoạt động phối hợp, đào tạo, tập huấn, các chương trình công tác bảo đảm an toàn thông tin khi có yêu cầu của tổ chức có thẩm quyền.

- Nhân lực, phổ biến, hướng dẫn: UBND xã cử cán bộ, công chức tham gia các lớp tập huấn, tuyên truyền do cấp trên tổ chức.

- Quản lý tài khoản, thiết bị, tài sản thông tin: Tài khoản người dùng, tài khoản quản trị được quản lý tách biệt và phân quyền theo chức năng, nhiệm vụ; tài khoản không hoạt động sau thời gian tối đa 45 ngày hoặc khi thay đổi nhân sự sẽ bị vô hiệu hóa; thiết bị mạng, máy trạm được kiểm kê, cập nhật danh sách tối thiểu 02 lần/năm; tài sản thông tin được phân loại theo mức độ nhạy cảm; không tự ý thay đổi, tháo lắp thiết bị khi chưa được phép.

- Quản lý rủi ro, ứng phó sự cố, sao lưu: Công tác xác định, đánh giá, xử lý rủi ro, phân loại và ứng cứu sự cố theo Quyết định số 05/2017/QĐ-TTg, sao lưu, khôi phục dữ liệu được thực hiện theo Quy chế; UBND xã duy trì đầu mối phối hợp với Công an tỉnh và các cơ quan chức năng trong hỗ trợ xử lý sự cố.

- Quản lý bên thứ ba: Danh sách nhà cung cấp sản phẩm, dịch vụ được lập và rà soát tối thiểu 01 lần/năm; đối với đơn vị cung cấp thiết bị, dịch vụ trong gói hợp đồng nâng cấp hệ thống, UBND xã quản lý phạm vi công việc, tài khoản, quyền truy cập theo nội dung hợp đồng và rà soát vấn đề bảo mật khi kết thúc hợp đồng; hệ thống không thuê đơn vị khác vận hành thay.

2. Triển khai các biện pháp kỹ thuật

- Bảo vệ hạ tầng mạng: Hệ thống WiFi tách VLAN với mạng nội bộ; 02 thiết bị tường lửa Fortinet FortiGate 60F kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, chặn các truy cập không được phép, chỉ cho phép kết nối được mã hóa, xác thực khi truy cập hoặc quản trị từ xa; tích hợp chức năng phòng chống xâm nhập (IPS), tự động cập nhật cơ sở dữ liệu dấu hiệu tấn công.

- Bảo vệ máy trạm, thiết bị đầu cuối: Máy trạm được cài đặt phần mềm phòng, chống mã độc theo phương án của hồ sơ cấp độ; quản lý tài khoản, phân quyền truy cập, tự động khóa phiên làm việc khi không thao tác; kiểm soát thiết bị lưu trữ ngoài; cập nhật hệ điều hành, phần mềm và bản vá bảo mật tối thiểu 01 lần/tháng, xử lý điểm yếu khi phát hiện. UBND xã không có hệ thống máy chủ.

- Bảo vệ phần mềm, ứng dụng: Người dùng truy cập các phần mềm dùng chung bằng tài khoản được cấp riêng, có phân quyền theo nhiệm vụ; thiết lập giới hạn thời gian chờ đóng phiên kết nối; nhật ký truy cập, đăng nhập quản trị được ghi nhận qua hệ thống tường lửa, lưu trữ tối thiểu 12 tháng và được rà soát định kỳ theo Quy chế.

- Bảo vệ dữ liệu: Quản lý quyền truy cập dữ liệu theo phân quyền; sao lưu định kỳ (hằng tháng hoặc khi thay đổi cấu hình) tập tin cấu hình thiết bị mạng và dữ liệu quan trọng, lưu bản sao tại nơi an toàn, kiểm tra khả năng khôi phục dữ liệu.

- Giám sát và phát hiện nguy cơ: Bật chức năng ghi và lưu nhật ký hoạt động trên tường lửa FortiGate, thiết bị chuyển mạch Cisco và thiết bị WiFi UniFi; theo dõi các cảnh báo nguy cơ do Công an tỉnh và cơ quan chức năng cung cấp, kịp thời kiểm tra, xử lý.

3. Công tác kiểm tra, giám sát và xử lý sự cố

- UBND xã tự kiểm tra, đánh giá việc thực hiện các biện pháp bảo đảm an toàn thông tin theo hồ sơ đã được phê duyệt; kết quả: các yêu cầu quản lý và kỹ thuật của cấp độ 2 đã được triển khai đầy đủ.

- Thường xuyên rà soát cấu hình thiết bị, cập nhật phần mềm, phát hiện và khắc phục lỗ hổng, điểm yếu bảo mật trên thiết bị mạng và máy trạm.

- Từ khi hệ thống được phê duyệt cấp độ đến nay, hệ thống chưa phát sinh sự cố an toàn thông tin nghiêm trọng.

- Việc kiểm tra phương án sao lưu, khôi phục dữ liệu và phương án ứng phó sự cố được thực hiện theo Quy chế bảo đảm an toàn thông tin của UBND xã.

- Các tồn tại phát hiện qua tự kiểm tra, qua cảnh báo của cơ quan chức năng đã được khắc phục theo hướng dẫn.

III. ĐÁNH GIÁ CHUNG

1. Kết quả đạt được

- Hệ thống thông tin Mạng nội bộ (LAN) đã được Công an tỉnh phê duyệt cấp độ 2; UBND xã đã hoàn thành việc triển khai toàn bộ phương án bảo đảm an toàn thông tin theo cấp độ 2 (cả biện pháp quản lý và biện pháp kỹ thuật), đáp ứng các yêu cầu theo hồ sơ đề xuất cấp độ đã được phê duyệt.

- Hệ thống vận hành ổn định, an toàn, phục vụ hiệu quả công tác chỉ đạo, điều hành của UBND xã.

- Đã ban hành Quy chế, phân công rõ đơn vị vận hành, đầu mối phối hợp và trách nhiệm của cán bộ, công chức.

2. Tồn tại, hạn chế

- Công chức phụ trách công nghệ thông tin, an toàn thông tin còn kiêm nhiệm nhiều lĩnh vực, chưa có cán bộ chuyên trách.

- Kinh phí dành cho duy trì, bảo trì và nâng cấp các giải pháp an toàn thông tin hằng năm còn hạn chế.

3. Khó khăn, vướng mắc

- Hạn chế về nhân lực chuyên trách an toàn thông tin cấp xã; điều kiện ngân sách cấp xã còn khó khăn; nhu cầu đầu tư, nâng cấp hạ tầng kỹ thuật ngày càng lớn.

IV. PHƯƠNG HƯỚNG, BIỆN PHÁP KHẮC PHỤC

Đề nghị Công an tỉnh tiếp tục hướng dẫn chuyên môn, hỗ trợ kỹ thuật, kịp thời cảnh báo nguy cơ mất an toàn thông tin; tổ chức các lớp tập huấn chuyên sâu cho công chức phụ trách an toàn thông tin cấp xã; quan tâm hỗ trợ điều kiện cần thiết về kinh phí, nhân lực cho cấp xã.

UBND xã Phạm Ngũ Lão trân trọng báo cáo Công an tỉnh Hưng Yên./.

Nơi nhận:
- Công an tỉnh Hưng Yên (để b/c);
- Chủ tịch, các PCT UBND xã;
- Lưu: VT, VHXH.

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

U.B.N.D XÃ PHẠM NGŨ LÃO HƯNG YÊN

Đặng Đức Lâm