

**ỦY BAN NHÂN DÂN
XÃ KIỀU PHÚ**

Số: /UBND-VP

V/v tăng cường công tác bảo đảm
an ninh mạng, an toàn thông tin.

**CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc**

Kiều Phú, ngày tháng năm 2025

Kính gửi:

- Đảng ủy, HĐND, UBNDTTQ và các Đoàn thể chính trị - Xã hội;
- Các cơ quan, Trường học, Đơn vị sự nghiệp trực thuộc.

Thực hiện Công văn số 6976/CAHN-PA05 ngày 06/10/2025 của Công an thành phố Hà Nội về việc tăng cường công tác bảo đảm an ninh mạng, an toàn thông tin. UBND xã Kiều Phú có ý kiến như sau:

Thời gian gần đây, tình trạng các hệ thống thông tin bị tấn công, chiếm quyền điều khiển, đánh cắp thông tin, dữ liệu cá nhân, diễn biến hết sức phức tạp gây ảnh hưởng nghiêm trọng đến an ninh mạng, an toàn thông tin. Thực hiện chức năng quản lý nhà nước về an ninh, an toàn thông tin mạng trên địa bàn xã Kiều Phú, UBND xã nhận thấy công tác bảo đảm an toàn thông tin, đặc biệt là công tác bảo vệ dữ liệu cá nhân, bí mật nhà nước chưa được chú trọng đúng mức. Việc quản trị, giám sát, vận hành, kiểm tra, rà soát các hệ thống thông tin, các thiết bị công nghệ thông tin chưa thường xuyên dẫn tới tình trạng các hệ thống, thiết bị chưa được cập nhật bản vá lỗi hồng bảo mật, bổ sung, thay thế, tạo điều kiện cho tin tặc khai thác, tấn công, xâm nhập, chiếm quyền điều khiển, cài mã độc hoặc sử dụng làm bàn đạp thực hiện các cuộc tấn công leo thang đặc quyền để truy xuất trái phép vào tài liệu nội bộ, thông tin thuộc danh mục bí mật nhà nước hoặc thông tin, dữ liệu cá nhân, dữ liệu nhạy cảm khác của các cá nhân, cơ quan, đơn vị, gây ảnh hưởng lớn đến an ninh mạng, an toàn thông tin mạng.

Từ tình hình trên, nhằm tăng cường công tác bảo đảm an ninh mạng, an toàn thông tin đối với các hệ thống thông tin trên địa bàn xã, UBND xã đề nghị các cơ quan, đơn vị triển khai một số nội dung sau:

1. Tăng cường công tác bảo đảm an ninh, an toàn hệ thống thông tin, mạng máy tính của đơn vị quản lý, vận hành.

- Thường xuyên, chủ động tự rà soát, kiểm tra, đánh giá hệ thống thông tin, các thiết bị mạng, bộ định tuyến kịp thời phát hiện những điểm yếu, lỗ hổng bảo mật.
- Không sử dụng mật khẩu tài khoản mặc định để đảm bảo an ninh mạng trong quá trình xây dựng, nâng cấp hệ thống thông tin, quản trị kết nối, chia sẻ dữ liệu nhất là quá trình chuyển giao, vận hành chính quyền địa phương 02 cấp, triển khai chuyển đổi số và nhiệm vụ Nghị quyết số 57-NQ/TW.
- Chủ động trong công tác quản lý, vận hành hệ thống, phân công cán bộ quản lý, quản trị cụ thể đối với hệ thống thông tin.

2. Đảm bảo máy tính tại đơn vị được cài đặt phần mềm diệt virus, phòng chống mã độc.

- Kiểm tra an ninh, an toàn thông tin đối với các máy tính, thiết bị trước khi đưa vào sử dụng theo quy định, cập nhật phiên bản mới nhất của hệ điều hành và các ứng dụng.

- Ban hành nội quy bảo vệ bí mật nhà nước, nội quy sử dụng máy tính, mạng máy tính tại cơ quan.

- Không sử dụng các hệ điều hành các thiết bị điện tử hiện không còn hỗ trợ cập nhật bản vá lỗ hổng bảo mật.

- Không soạn thảo, lưu trữ, trao đổi thông tin, tài liệu chứa bí mật nhà nước trên các máy tính có kết nối Internet.

3. Thường xuyên rà soát bảo mật tài khoản quản trị viên của các hệ thống, có giải pháp bảo đảm, không để lộ tài khoản mật khẩu truy cập hệ thống thông tin.

- Không sử dụng cùng một mật khẩu cho nhiều tài khoản khác nhau, không chia sẻ thông tin tài khoản, mật khẩu truy cập hệ thống cho người khác trái quy định.

- Đặt mật khẩu truy cập máy tính, đảm bảo mật khẩu đủ mạnh.

- Không sử dụng mật khẩu mặc định truy cập hệ thống, sử dụng mật khẩu truy cập đủ mạnh có chữ hoa, chữ thường, số và ký tự đặc biệt.

4. Thường xuyên kiểm tra, rà soát công tác chấp hành các quy định về bảo đảm an ninh mạng, an toàn thông tin, kịp thời phát hiện những sơ hở, hạn chế, thiếu sót trong công tác bảo mật an toàn thông tin, dữ liệu. Đề xuất giải pháp sửa đổi, bổ sung, thay thế cho phù hợp và xử lý nghiêm theo quy định nếu phát hiện vi phạm.

5. Rà soát, thay thế, bổ sung hồ sơ; xây dựng, thẩm định, phê duyệt hồ sơ cấp độ an toàn thông tin đối với các hệ thống thông tin quản lý, vận hành theo các quy định của pháp luật và các hướng dẫn có liên quan.

6. Phổ biến đến toàn thể cán bộ, nhân viên đơn vị, người dân, doanh nghiệp để nâng cao cảnh giác với các thủ đoạn của các đối tượng tội phạm lợi dụng việc thông tin cá nhân của các cá nhân, doanh nghiệp bị lộ lọt để thực hiện hoạt động lừa đảo hoặc vi phạm pháp luật khác.

Quá trình thực hiện nếu có khó khăn, vướng mắc đề nghị các đơn vị trao đổi về Văn phòng UBND xã để phối hợp, xử lý. UBND xã trao đổi để quý cơ quan phối hợp, thực hiện./.

Nơi nhận:

- Như đề gửi;
- Chủ tịch UBND xã; (để b/c)
- Các PCT UBND xã;
- Lưu: VT.

TM. ỦY BAN NHÂN DÂN

KT. CHỦ TỊCH

PHÓ CHỦ TỊCH

Kiều Thị Nga