

Số: /KH-UBND

Khánh Xuân, ngày tháng 7 năm 2025

KẾ HOẠCH

Đảm bảo an ninh an toàn an ninh mạng và bảo vệ bí mật nhà nước trên không gian mạng khắc phục các lỗ hổng bảo mật trên máy tính

Căn cứ theo kế hoạch số 02/KH-UBND ngày 15/7/2025 của Ủy ban nhân dân xã Khánh Xuân thực hiện công tác Bảo vệ nhà nước.

Ủy ban nhân dân xã Khánh Xuân xây dựng kế hoạch đảm bảo an ninh mạng và bảo vệ bí mật nhà nước trên không gian mạng, khắc phục các lỗ hổng bảo mật trên máy tính với các nội dung sau:

I. MỤC ĐÍCH YÊU CẦU

1. Mục đích

- Nâng cao năng lực bảo vệ an toàn thông tin mạng của UBND xã, đặc biệt là hệ thống máy tính phục vụ công vụ.
- Chủ động phát hiện, xử lý, khắc phục kịp thời các lỗ hổng bảo vệ bí mật nhà nước không bị lộ lọt, bị lợi dụng hoặc phá hoại trên không gian mạng.
- Tuân thủ các quy định của pháp luật về an ninh mạng, an toàn thông tin và bảo vệ bí mật nhà nước.

2. Yêu cầu

- Thực hiện nghiêm túc các quy định pháp luật về bảo vệ bí mật nhà nước, an toàn thông tin mạng.
- Triển khai đồng bộ nghiêm túc các biện pháp kỹ thuật và hành chính.
- Phân công rõ trách nhiệm cho từng bộ phận, cá nhân.
- Đảm bảo không làm gián đoạn hoạt động của các hệ thống thông tin trong quá trình rà soát, xử lý.

II. NỘI DUNG THỰC HIỆN

1. Rà soát, đánh giá hiện trạng an toàn thông tin hệ thống máy tính

- Kiểm tra toàn bộ máy tính đang sử dụng tại UBND xã đặc biệt là máy tính có kết nối mạng internet, máy lưu trữ văn bản mật, tài liệu nội bộ.

- Phát hiện các phần mềm độc hại, phần mềm không rõ nguồn gốc, các cấu hình không an toàn.

2. Phát hiện và xử lý lỗ hổng bảo mật

- Cập nhật hệ thống điều hành, phần mềm ứng dụng lên phiên bản mới nhất.
- Gỡ bỏ các phần mềm, tiện ích không cần thiết, không rõ nguồn gốc.
- Cài đặt phần mềm diệt virus, tường lửa, mã hóa dữ liệu đối với máy tính lưu trữ thông tin nhạy cảm.
- Thiết lập tài khoản người dùng hợp lý (mỗi cá nhân một tài khoản, mật khẩu mạnh, định kỳ thay đổi mật khẩu).
- Không sử dụng thiết bị USB, thiết bị lưu trữ di động không rõ nguồn gốc vào máy tính công vụ.

3. Bảo vệ bí mật nhà nước

- Phân loại thông tin, văn bản theo quy định về bảo vệ bí mật nhà nước.
- Không lưu văn bản mật trên máy tính có kết nối mạng internet nếu không có phần mềm bảo vệ chuyên dụng.
- Không gửi chia sẻ văn bản nội bộ qua email cá nhân hoặc các nền tảng mạng xã hội.

4. Tập huấn, tuyên truyền nâng cao nhận thức

- Tổ chức tập huấn cho các cán bộ, công chức về kỹ năng sử dụng an toàn máy tính, nhận biết các hành vi lừa đảo qua mạng, mã độc...
- Cập nhật các văn bản pháp luật mới về an ninh mạng và bảo vệ bí mật nhà nước.

III. PHÂN CÔNG THỰC HIỆN

STT	Bộ Phận/Cá Nhân	Nhiệm Vụ
1	Văn phòng HĐND – UBND	Chủ trì rà soát, cập nhật hệ thống, cài đặt phần mềm bảo mật, phối hợp đơn vị chuyên môn xử lý sự cố.
2	Phòng văn hóa – xã hội	Phối hợp tập huấn, truyền thông về an toàn thông tin.
3	Trưởng các phòng chuyên môn, ban ngành	Quản lý, giám sát việc sử dụng máy tính của cán bộ, đảm bảo thực hiện nghiêm các quy định.

4	Toàn thể cán bộ, công chức	Tuân thủ quy định về sử dụng máy tính, xử lý thông tin, không tự ý cài đặt phần mềm, truy cập trang web không an toàn.
5	Công an xã	Phối hợp bảo vệ an ninh mạng, xử lý vi phạm.

IV. TỔ CHỨC THỰC HIỆN

Ủy ban nhân dân xã giao Văn phòng chủ trì, phối hợp với các bộ phận triển khai kế hoạch. Tăng cường kiểm tra, đánh giá định kỳ việc thực hiện, báo cáo kết quả về Ủy ban nhân dân xã theo quy định hoặc khi có yêu cầu./.

Nơi nhận:

- Thường trực Đảng ủy xã;
- Thường trực HĐND xã;
- Chủ tịch, các PCT UBND xã;
- Công an xã;
- Các phòng chuyên môn, ban ngành;
- Lưu: VT.

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**

Tô Đức Bình