

**ỦY BAN NHÂN DÂN
XÃ ĐẮK HÀ**

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

Số: /UBND-NC

Đắk Hà, ngày tháng năm 2025

Về việc tăng cường các biện
pháp phòng, chống tấn công
mạng, gián điệp mạng

Kính gửi: Các cơ quan, đơn vị¹.

Hiện nay, tình hình an ninh mạng đang diễn biến ngày càng phức tạp, tiềm ẩn nguy cơ mất an ninh mạng, an toàn thông tin, lộ, mất bí mật nhà nước trên không gian mạng. Đặc biệt là các hành vi tấn công mạng, gián điệp mạng, đánh cắp thông tin qua các hình thức tinh vi như: giả mạo tài khoản, phát tán mã độc, phần mềm gián điệp, xâm nhập hệ thống thông tin công vụ,... Hoạt động tấn công mạng, gián điệp mạng không chỉ đe dọa xâm phạm an ninh cơ sở hạ tầng trọng yếu, lộ, mất bí mật Nhà nước mà còn gây thiệt hại nặng nề về tài chính, danh tiếng, độ tin cậy của cơ quan, tổ chức, doanh nghiệp bị tấn công.

Thực hiện Công văn số 33/UBND-NC, ngày 31/7/2025 của UBND Tỉnh Quảng Ngãi về tăng cường các biện pháp phòng, chống tấn công mạng, gián điệp mạng; nhằm chủ động phòng ngừa, kịp thời phát hiện và ngăn chặn các hành vi nêu trên, Ủy ban nhân dân xã yêu cầu các cơ quan, đơn vị theo chức năng, nhiệm vụ thực hiện một số nội dung sau:

1. Tiếp tục quán triệt, triển khai thực hiện nghiêm túc các quy định của pháp luật, ý kiến chỉ đạo của Ban Thường vụ Tỉnh ủy, UBND Tỉnh và Đảng ủy xã về công tác bảo đảm an toàn thông tin, an ninh mạng, bảo vệ bí mật nhà nước. Phát huy vai trò, trách nhiệm của Thủ trưởng các cơ quan, đơn vị đối với công tác bảo đảm an toàn thông tin, an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng tại cơ quan, đơn vị mình. Xây dựng và hoàn thiện quy trình quản lý, cấp phát, thu hồi, sử dụng tài khoản công vụ, tài khoản truy cập hệ thống thông tin phục vụ hành chính công, dịch vụ công, một cửa. Xử lý nghiêm tập thể, cá nhân vi phạm quy định, quy chế để xảy ra tình trạng mất an toàn thông tin, an ninh mạng, lộ, mất thông tin, tài liệu nội bộ, bí mật nhà nước.

Tổ chức tuyên truyền, phổ biến đến cán bộ, công chức, viên chức và nhân dân về các nguy cơ tấn công mạng và biện pháp phòng tránh. Khuyến khích sử dụng phần mềm diệt virus, không truy cập các đường link lạ, không mở tệp đính kèm không rõ nguồn gốc.

2. Chủ động tự rà soát, triển khai các biện pháp khắc phục hạn chế, khuyết điểm trong công tác bảo đảm an toàn thông tin mạng, an ninh mạng, bảo vệ bí mật nhà nước trên không gian mạng tại cơ quan, đơn vị và lĩnh vực phụ trách. Kiểm

¹ Phòng Kinh tế; phòng Văn hoá - Xã hội; Trung tâm phục vụ hành chính công; Trung tâm Văn hóa - Thể thao - Du lịch và Truyền thông xã; Trung tâm dịch vụ nông nghiệp xã; Ban Quản lý dự án và dịch vụ công ích xã; Ban Chỉ huy quân sự xã; Công an xã; Ủy ban Mặt trận Tổ quốc Việt Nam và các tổ chức đoàn thể xã.

tra, cập nhật phần mềm bảo mật cho toàn bộ thiết bị công vụ. Thiết lập chế độ sao lưu dữ liệu định kỳ, bảo vệ mật khẩu nghiêm ngặt, không chia sẻ thông tin tài khoản.

3. Mỗi cơ quan, đơn vị cần cử ít nhất 01 cán bộ phụ trách công nghệ thông tin để theo dõi, phát hiện và báo cáo kịp thời các dấu hiệu bất thường về an ninh mạng. Tham gia đầy đủ các buổi tập huấn, bồi dưỡng chuyên môn khi có kế hoạch của cấp trên. Rà soát, phân loại, đánh giá toàn bộ hệ thống thông tin lại cơ quan, đơn vị với từng cấp độ an toàn thông tin theo Nghị định số 85/2016/NĐ-CP của Chính phủ; triển khai thay thế các giải pháp đảm bảo an ninh mạng đã lỗi thời bằng các giải pháp, thiết bị mới; trang bị thêm các giải pháp phòng, chống virus, mã độc.

4. Công an xã chủ trì, hướng dẫn, đôn đốc các cơ quan, đơn vị triển khai nghiêm túc các nhiệm vụ được giao tại công văn này; báo cáo kết quả thực hiện về Công an tỉnh và UBND xã khi có yêu cầu.

Đề nghị các cơ quan, đơn vị thực hiện nghiêm túc. Trong quá trình thực hiện, phát sinh vướng mắc, bất cập hoặc liên quan đến tình hình an ninh, trật tự, kịp thời báo cáo UBND xã để theo dõi, chỉ đạo./.

Nơi nhận:

- Như trên (t/h);
- UBND tỉnh (b/c);
- Thường trực Đảng ủy (b/c);
- Thường trực HĐND xã (b/c);
- Đ/c Chủ tịch và các Phó Chủ tịch;
- LĐ, CVVP;
- Lưu: VT.

**TM. ỦY BAN NHÂN DÂN
CHỦ TỊCH**

Nguyễn Minh Vương