

Số: 1994 /UBND-VP
V/v tăng cường công tác bảo
đảm an ninh mạng trong thời
gian nghỉ Lễ Quốc khánh 02/9

Sơn Kỳ, ngày 28 tháng 8 năm 2026

Kính gửi:

- Công an xã;
- Các cơ quan đơn vị, sự nghiệp thuộc UBND xã.

Thực hiện Công văn số 6583/CAT-ANM ngày 27 tháng 8 năm 2026 của Công an tỉnh Quảng Ngãi về việc tăng cường công tác bảo đảm an ninh mạng trong thời gian nghỉ Lễ Quốc khánh 02/9; Ủy ban nhân dân xã yêu cầu Thủ trưởng các cơ quan, đơn vị và cán bộ, công chức, viên chức, người lao động nghiêm túc triển khai các nội dung sau:

1. Tăng cường hoạt động bảo đảm an ninh mạng

a) Quán triệt, thực hiện nghiêm Quy chế bảo đảm an ninh mạng ban hành kèm theo Quyết định số 132/2026/QĐ-UBND ngày 20 tháng 7 năm 2026 của Ủy ban nhân dân tỉnh. Người đứng đầu chịu trách nhiệm trực tiếp đối với hệ thống thông tin, thiết bị, tài khoản và dữ liệu thuộc phạm vi quản lý.

b) Phân công cán bộ đầu mối, bảo đảm liên lạc thông suốt trong thời gian nghỉ. Đơn vị trực tiếp quản trị, vận hành máy chủ hoặc hệ thống thông tin phải bố trí trực kỹ thuật, giám sát 24/7, kịp thời tiếp nhận, xử lý cảnh báo.

c) Hoàn thành việc kiểm tra, rà soát trước thời điểm bắt đầu kỳ nghỉ, tập trung vào các nội dung:

- Kiểm tra máy chủ, máy trạm, thiết bị mạng, đường truyền, ứng dụng và dịch vụ; cập nhật hệ điều hành, phần mềm, bản vá bảo mật; quét, bóc gỡ mã độc; xử lý điểm yếu, lỗ hổng và địa chỉ IP thuộc danh sách mạng Botnet theo cảnh báo.

- Đối với hệ thống do đơn vị trực tiếp quản lý, vận hành, rà soát biện pháp bảo vệ tương ứng với cấp độ theo TCVN 14423:2026; kiểm tra tường lửa, phòng chống xâm nhập, mã độc, quyền truy cập từ xa và nhật ký hệ thống.

- Sao lưu dữ liệu quan trọng, kiểm tra khả năng khôi phục; khóa tài khoản không còn sử dụng hoặc không rõ chủ thể; rà soát quyền truy cập theo đúng nhiệm vụ được giao.

d) Thay ngay mật khẩu yếu, đã sử dụng lâu hoặc có dấu hiệu lộ lọt. Mật khẩu phải có ít nhất 08 ký tự, gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt; không dùng chung tài khoản, chia sẻ mật khẩu, mã xác thực hoặc lưu mật khẩu trên trình duyệt; kích hoạt xác thực đa yếu tố khi hệ thống hỗ trợ.

e) Cảnh giác với thư điện tử, đường dẫn, tệp đính kèm, mã QR, cuộc gọi, tin nhắn không rõ nguồn gốc; không tự ý cài đặt phần mềm, kết nối thiết bị vào mạng nội bộ hoặc vô hiệu hóa giải pháp bảo mật; không xử lý tài liệu bí mật nhà nước trên thiết bị có kết nối Internet trái quy định; không cung cấp dữ liệu cá nhân, tài khoản, mã xác thực cho tổ chức, cá nhân không có thẩm quyền.

2. Công an xã: Chủ trì tham mưu, hướng dẫn, kiểm tra, theo dõi tình hình; tiếp nhận, xác minh, xử lý ban đầu và liên hệ Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao - Công an tỉnh khi sự cố vượt quá khả năng xử lý tại chỗ.

3. Phòng Văn hóa - Xã hội: Tham mưu tổ chức triển khai, theo dõi, đôn đốc các yêu cầu bảo đảm an ninh mạng trong ứng dụng công nghệ thông tin, chuyển đổi số; phối hợp Công an xã tổng hợp, tham mưu báo cáo khi có yêu cầu.

4. Văn phòng HĐND và UBND xã: Rà soát hạ tầng mạng, thiết bị, tài khoản Hệ thống quản lý văn bản và điều hành, thư điện tử công vụ, chữ ký số và các hệ thống được giao; bảo đảm thông tin chỉ đạo, điều hành, liên lạc trong thời gian nghỉ.

5. Trung tâm Phục vụ hành chính công xã: Bảo vệ thiết bị, tài khoản, dữ liệu trên các hệ thống giải quyết thủ tục hành chính; kiểm soát quyền truy cập, đăng xuất tài khoản khi không sử dụng, không lưu mật khẩu trên trình duyệt; báo ngay hoạt động truy cập, khai thác dữ liệu bất thường.

6. Trung tâm Cung ứng dịch vụ công ích xã: Trực tiếp kiểm tra, quản lý, vận hành an toàn hệ thống truyền thanh ứng dụng công nghệ thông tin - viễn thông, bảng tin điện tử, thiết bị, tài khoản và nền tảng được giao; theo dõi dấu hiệu bất thường, bảo vệ nội dung đăng, phát; thực hiện tuyên truyền, cảnh báo theo nội dung được cung cấp.

7. Phòng Kinh tế: Phối hợp tham mưu sửa chữa, thay thế thiết bị và kinh phí khắc phục sự cố khi phát sinh, bảo đảm đúng thẩm quyền, dự toán và quy định.

8. Trạm Y tế xã, các cơ sở giáo dục thuộc UBND xã: Rà soát hệ thống chuyên ngành, cơ sở dữ liệu, máy tính, thiết bị mạng, tài khoản và dữ liệu cá nhân thuộc phạm vi quản lý; thực hiện các biện pháp tại mục 1 Công văn này.

9. Xử lý và báo cáo sự cố

a) Khi phát hiện tấn công mạng, mã độc, mất quyền kiểm soát tài khoản, lộ lọt dữ liệu hoặc hoạt động bất thường, đơn vị phải kích hoạt phương án ứng cứu; cô lập thiết bị bị ảnh hưởng; bảo toàn hiện trạng, nhật ký; không tự ý xóa dữ liệu, cài đặt lại hệ điều hành hoặc làm mất dấu vết khi chưa có hướng dẫn.

b) Báo ngay người đứng đầu đơn vị, Công an xã và Ủy ban nhân dân xã (qua Văn phòng HĐND&UBND xã). Trường hợp vượt khả năng xử lý tại chỗ, Công an xã báo cáo Công an tỉnh, liên hệ các đầu mối tại Công văn số 6583/CAT-ANM; không chờ hoàn thiện báo cáo bằng văn bản mới thông tin sự cố.

c) Báo cáo đột xuất diễn biến, biện pháp xử lý, kết quả khắc phục theo yêu cầu; tiếp tục theo dõi, không đưa hệ thống trở lại hoạt động khi chưa bảo đảm an toàn.

Yêu cầu các cơ quan, đơn vị nghiêm túc triển khai thực hiện./.

Nơi nhận:

- Như trên;
- Thường trực Đảng ủy;
- Chủ tịch các PCT UBND xã;
- Lưu: VT, VP.



CHỦ TỊCH

Trần Đình Trân