ỦY BAN NHÂN DÂN XÃ QUỲNH PHỤ	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do- Hạnh phúc
Số: 855 /UBND-PVHXH	*Quỳnh Phụ, ngày 23 tháng 9 năm 2026*

V/v tăng cường công tác bảo đảm an ninh, an toàn hệ thống thông tin trong quá trình triển khai thực hiện Nghị quyết số 57-NQ/TW

Kính gửi:
- Các cơ quan, đơn vị chuyên môn thuộc UBND xã.
- Công an xã.

Thực hiện Công văn số 7561/CAT-PA05 ngày 21/9/2026 về việc tăng cường công tác bảo đảm an ninh, an toàn hệ thống thông tin trong quá trình triển khai thực hiện Nghị quyết số 57-NQ/TW; nhằm chủ động phòng ngừa nguy cơ mất, hư hỏng, thay đổi, sao chép hoặc lộ lọt dữ liệu; ngăn chặn việc sử dụng trái phép tài khoản quản trị, cài đặt phần mềm không rõ nguồn gốc hoặc duy trì các phương thức truy cập từ xa không được kiểm soát trong quá trình sửa chữa, bảo trì, nâng cấp, thay thế thiết bị, cài đặt lại phần mềm, cấu hình hệ thống và hỗ trợ kỹ thuật, Ủy ban nhân dân xã Quỳnh Phụ yêu cầu các cơ quan, đơn vị nghiêm túc thực hiện các nội dung sau:

1. Thực hiện sao lưu dữ liệu trước khi sửa chữa, bảo trì, nâng cấp

- Trước khi sửa chữa, nâng cấp, cài đặt lại hệ điều hành, phần mềm, thay thế thiết bị hoặc thực hiện các thao tác có khả năng ảnh hưởng đến dữ liệu, phải thực hiện sao lưu đầy đủ dữ liệu quan trọng.

- Tùy đặc điểm từng hệ thống, nội dung sao lưu phải bao gồm tối thiểu: cơ sở dữ liệu; hồ sơ, tài liệu điện tử; cấu hình hệ thống; cấu hình thiết bị mạng; tệp cấu hình phần mềm; tài khoản và thông tin cần thiết phục vụ khôi phục; nhật ký hệ thống và các dữ liệu cần thiết khác.

- Ưu tiên áp dụng quy tắc sao lưu 3-2-1: duy trì ít nhất 03 bản sao, trên 02 thiết bị/lưu trữ khác nhau và 01 bản ở vị trí độc lập; không để bản sao lưu duy nhất trên chính thiết bị hoặc cùng hệ thống đang được sửa chữa.

- Sau khi sao lưu phải kiểm tra khả năng đọc, tính đầy đủ và khả năng khôi phục của dữ liệu; không coi việc sao lưu là hoàn thành nếu chưa kiểm tra khả năng phục hồi.

2. Kiểm tra, ghi nhận hiện trạng và phê duyệt phương án trước khi sửa chữa

- Trước khi bàn giao thiết bị hoặc hệ thống cho cán bộ kỹ thuật, doanh nghiệp hoặc cá nhân bên ngoài, phải lập biên bản hoặc ghi nhận hiện trạng. Nội dung tối thiểu gồm: thiết bị/hệ thống được sửa chữa; tình trạng hoạt động; dữ liệu đang lưu trữ; tài khoản đang sử dụng; phần mềm đang cài đặt; kết nối mạng; lỗi, sự cố đã phát hiện; đơn vị/cá nhân thực hiện sửa chữa và phạm vi quyền truy cập

được cấp.

- Đối với hệ thống có dữ liệu quan trọng, dữ liệu cá nhân, dữ liệu nghiệp vụ hoặc dữ liệu phục vụ quản lý nhà nước, phương án sửa chữa, bảo trì, nâng cấp phải được người có thẩm quyền xem xét, chấp thuận trước khi thực hiện.

3. Kiểm soát chặt chẽ việc tiếp cận hệ thống và dữ liệu của đơn vị kỹ thuật

- Xác định rõ danh tính cá nhân được phép tiếp cận hệ thống, thiết bị và dữ liệu; chỉ cấp quyền truy cập trong phạm vi tối thiểu cần thiết để thực hiện công việc, không cấp quyền quản trị toàn bộ nếu không thực sự cần thiết.

- Không cung cấp tài khoản quản trị dùng chung hoặc mật khẩu của cán bộ quản trị cho đơn vị sửa chữa nếu có thể cấp tài khoản riêng. Trường hợp hỗ trợ từ xa, chỉ cho phép kết nối trong thời gian thực hiện công việc và phải có cán bộ có thẩm quyền giám sát.

- Hạn chế tối đa việc sao chép dữ liệu ra khỏi hệ thống. Trường hợp bắt buộc phải sao chép để xử lý kỹ thuật phải xác định rõ loại dữ liệu, phạm vi dữ liệu, thiết bị lưu trữ sử dụng; không sử dụng thiết bị lưu trữ cá nhân, không tự ý đưa dữ liệu lên dịch vụ lưu trữ trực tuyến; sau khi hoàn thành phải thu hồi, xóa hoặc hủy dữ liệu tạm theo quy định.

4. Kiểm soát phần mềm, tài khoản và kết nối trong, sau quá trình sửa chữa

- Không sử dụng phần mềm không rõ nguồn gốc, phần mềm bẻ khóa hoặc công cụ điều khiển từ xa không được kiểm soát. Mọi phần mềm, tiện ích hoặc công cụ kỹ thuật cài đặt phục vụ sửa chữa phải xác định được nguồn gốc, mục đích, thời gian sử dụng và phải gỡ bỏ khi không còn nhu cầu.

- Sau khi hoàn thành sửa chữa, nâng cấp hoặc khắc phục sự cố phải: thay đổi mật khẩu các tài khoản quản trị đã sử dụng; rà soát toàn bộ tài khoản, đặc biệt là tài khoản quản trị/hỗ trợ kỹ thuật; khóa hoặc xóa tài khoản không còn nhu cầu; rà soát phần mềm điều khiển từ xa, dịch vụ truy cập từ xa và các kết nối được thiết lập trong quá trình sửa chữa.

- Kiểm tra lại cấu hình hệ thống, thiết bị mạng và quyền truy cập trước khi đưa hệ thống trở lại hoạt động bình thường.

5. Kiểm tra, xác nhận hệ thống sau khi khắc phục

- Sau khi hoàn thành sửa chữa phải kiểm tra và xác nhận: dữ liệu còn đầy đủ, nguyên vẹn; phần mềm hoạt động bình thường; tài khoản không bị thay đổi trái phép; không phát sinh tài khoản mới, phần mềm, dịch vụ hoặc kết nối bất thường; thiết bị không có kết nối mạng bất thường; quyền truy cập phù hợp với trạng thái được phê duyệt.

- Đối với hệ thống quan trọng, phải kiểm tra nhật ký hoạt động trong và sau thời gian sửa chữa để kịp thời phát hiện thao tác bất thường; lập biên bản hoàn thành và lưu hồ sơ phục vụ kiểm tra, đối chiếu khi cần thiết.

6. Xây dựng và thực hiện thống nhất quy trình sửa chữa, bảo trì, khắc phục hệ thống thông tin

- Các cơ quan, đơn vị căn cứ điều kiện thực tế để xây dựng hoặc bổ sung vào quy chế nội bộ quy trình kiểm soát hoạt động sửa chữa, bảo trì, nâng cấp, khắc phục hệ thống thông tin. Quy trình tối thiểu gồm 12 bước: (1) tiếp nhận và xác định sự cố; (2) đánh giá mức độ ảnh hưởng; (3) sao lưu dữ liệu; (4) ghi nhận hiện trạng; (5) phê duyệt phương án sửa chữa; (6) cấp quyền truy cập cho cán bộ/đơn vị kỹ thuật; (7) thực hiện sửa chữa; (8) kiểm tra, đánh giá sau sửa chữa; (9) thu hồi quyền truy cập của đơn vị kỹ thuật; (10) thay đổi mật khẩu tài khoản quản trị; (11) kiểm tra và xác nhận dữ liệu; (12) lập biên bản hoàn thành và lưu hồ sơ.

7. Tổ chức thực hiện

- Phòng Văn hóa - Xã hội là đầu mối tham mưu UBND xã hướng dẫn, đôn đốc các cơ quan, đơn vị thực hiện các yêu cầu nêu trên; tổng hợp khó khăn, vướng mắc và báo cáo UBND xã để chỉ đạo xử lý.

- Công an xã chủ trì, phối hợp Phòng Văn hóa - Xã hội hướng dẫn công tác bảo đảm an ninh mạng, an toàn thông tin; khi phát hiện dấu hiệu bất thường, nghi ngờ mất dữ liệu, lộ lọt thông tin, cài đặt mã độc hoặc truy cập trái phép, kịp thời tham mưu tạm dừng các thao tác không cần thiết, bảo toàn hiện trạng và phối hợp cơ quan chức năng kiểm tra, xác minh, xử lý.

- Thủ trưởng các cơ quan, đơn vị chịu trách nhiệm tổ chức quán triệt đến cán bộ, công chức, viên chức, người lao động có liên quan; trực tiếp chịu trách nhiệm nếu để xảy ra mất an ninh, an toàn thông tin do không thực hiện hoặc thực hiện không đầy đủ các yêu cầu kiểm soát trong quá trình sửa chữa, bảo trì, nâng cấp, khắc phục sự cố.

- Đối với các hệ thống có chứa dữ liệu quan trọng, dữ liệu cá nhân hoặc dữ liệu phục vụ hoạt động quản lý nhà nước, phải áp dụng biện pháp kiểm soát chặt chẽ hơn và duy trì bản sao lưu độc lập; định kỳ kiểm tra khả năng khôi phục dữ liệu.

Nhận công văn, yêu cầu các phòng chuyên môn, Trung tâm Phục vụ hành chính công, công an xã nghiêm túc triển khai thực hiện./.

Nơi nhận:
- Như kính gửi;
- Chủ tịch, các PCT UBND xã;
- Lưu: VT, PVHXH, PTN.

KT. CHỦ TỊCH
PHÓ CHỦ TỊCH

U.B.N.D XÃ QUỲNH PHỤ T.HƯNG YÊN

Bùi Thị Nhẫn