

Số: 938 /UBND-VHXXH

Hiệp Cường, ngày 30 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 phòng, đơn vị thuộc UBND xã

Căn cứ công văn số 7561/CAT-PAT ngày 21/09/2026 của Công an tỉnh Hưng Yên 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.

Thực hiện chủ trương đẩy mạnh chuyển đổi số, ứng dụng khoa học, công nghệ và công nghệ thông tin trong hoạt động quản lý nhà nước theo tinh thần Nghị quyết số 57-NQ/TW của Bộ Chính trị, thời gian qua, các đơn vị đã triển khai, khai thác nhiều hệ thống thông tin, phần mềm, cơ sở dữ liệu và thiết bị công nghệ thông tin phục vụ công tác chuyên môn, quản lý, điều hành. Trong quá trình vận hành, việc phát sinh các yêu cầu khắc phục sự cố, sửa chữa, bảo trì, nâng cấp, thay thế thiết bị, cài đặt lại phần mềm, cấu hình hệ thống hoặc thuê đơn vị kỹ thuật hỗ trợ là cần thiết để duy trì hoạt động ổn định của hệ thống.

Tuy nhiên, đây cũng là thời điểm tiềm ẩn nhiều nguy cơ mất an ninh, an toàn thông tin nếu không có biện pháp kiểm soát phù hợp. Quá trình sửa chữa, khắc phục có thể dẫn đến việc mất, hư hỏng hoặc thay đổi dữ liệu; dữ liệu có thể bị sao chép, lộ lọt; tài khoản quản trị có thể bị sử dụng trái phép; thiết bị có thể bị cài đặt phần mềm không rõ nguồn gốc hoặc để lại tài khoản truy cập từ xa. Đặc biệt, trường hợp có sự tham gia của đơn vị, cá nhân bên ngoài trong quá trình sửa chữa, việc kiểm soát quyền tiếp cận hệ thống và dữ liệu cần được đặc biệt chú trọng. Để hạn chế nguy cơ mất an ninh, an toàn hệ thống thông tin và bảo đảm khả năng khôi phục hoạt động khi xảy ra sự cố, UBND xã Hiệp Cường yêu cầu các phòng, đơn vị thực hiện một số nội dung sau:

I. THỰC HIỆN SAO LƯU DỮ LIỆU TRƯỚC KHI KHẮC PHỤC, SỬA CHỮA

1. Trước khi tiến hành 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, cần thực hiện sao lưu đầy đủ dữ liệu quan trọng.

2. Việc sao lưu cần bao gồm, tùy theo đặc điểm của từng hệ thống:

- Cơ sở dữ liệu;
- Hồ sơ, tài liệu điện tử;
- Cấu hình hệ thống;
- Cấu hình thiết bị mạng;
- Các tệp cấu hình phần mềm;

- Tài khoản và thông tin cần thiết phục vụ khôi phục hệ thống;
- Nhật ký hệ thống và các dữ liệu cần thiết khác.

3. Áp dụng quy tắc 3-2-1 trong sao lưu dữ liệu giúp bảo vệ an toàn cho dữ liệu bằng cách duy trì ít nhất 3 bản sao trên 2 thiết bị khác nhau và 1 bản ở vị trí khác (không để bản sao lưu duy nhất ngay trên thiết bị đang được sửa chữa hoặc trên cùng hệ thống có nguy cơ xảy ra sự cố); bảo đảm bản sao lưu có khả năng sử dụng để khôi phục khi dữ liệu gốc bị mất, hỏng hoặc mã hóa.

4. Sau khi hoàn thành sao lưu cần kiểm tra khả năng đọc, tính đầy đủ và khả năng khôi phục của dữ liệu; không chỉ thực hiện sao lưu nhưng không kiểm tra khả năng phục hồi.

II. KIỂM TRA VÀ GHI NHẬN HIỆN TRẠNG TRƯỚC KHI SỬA CHỮA

Trước khi bàn giao thiết bị hoặc hệ thống cho đơn vị kỹ thuật, đề nghị lập biên bản hoặc ghi nhận hiện trạng, trong đó xác định:

- Thiết bị, hệ thống được sửa chữa;
- Tình trạng hoạt động trước khi sửa chữa;
- Dữ liệu đang được lưu trữ;
- Các tài khoản đang được sử dụng;
- Các phần mềm đang cài đặt;
- Các kết nối mạng đang tồn tại;
- Các lỗi, sự cố đã phát hiện;
- Đơn vị, cá nhân thực hiện sửa chữa;

Phạm vi quyền truy cập được cấp cho đơn vị kỹ thuật.

Việc ghi nhận hiện trạng nhằm tạo cơ sở đối chiếu, xác định trách nhiệm và phát hiện các thay đổi bất thường sau khi hoàn thành việc sửa chữa.

III. KIỂM SOÁT VIỆC TIẾP CẬN HỆ THỐNG CỦA ĐƠN VỊ KỸ THUẬT

Trường hợp thuê doanh nghiệp hoặc cá nhân bên ngoài thực hiện sửa chữa, đề nghị:

1. Xác định rõ danh tính cá nhân được phép tiếp cận hệ thống, thiết bị và dữ liệu.
2. Chỉ cấp quyền truy cập trong phạm vi cần thiết để thực hiện công việc; không cấp quyền quản trị toàn bộ hệ thống nếu không thực sự cần thiết.
3. Không cung cấp tài khoản quản trị dùng chung hoặc mật khẩu của cán bộ quản trị cho đơn vị sửa chữa khi có phương án cấp tài khoản riêng.
4. Đối với việc hỗ trợ từ xa, chỉ cho phép kết nối trong thời gian thực hiện công việc và phải được cán bộ có thẩm quyền của các đơn vị kiểm soát.
5. Sau khi hoàn thành công việc phải thu hồi tài khoản, quyền truy cập, mật khẩu và các phương thức truy cập từ xa đã cấp cho đơn vị kỹ thuật.

IV. KIỂM SOÁT DỮ LIỆU TRONG QUÁ TRÌNH SỬA CHỮA

Hạn chế tối đa việc sao chép dữ liệu ra khỏi hệ thống trong quá trình sửa chữa. Trường hợp bắt buộc phải sao chép dữ liệu để phục vụ xử lý kỹ thuật:

- Xác định rõ loại dữ liệu, phạm vi dữ liệu được sao chép;
- Chỉ sao chép dữ liệu thực sự cần thiết;
- Không sử dụng thiết bị lưu trữ cá nhân để sao chép dữ liệu;
- Không tự ý đưa dữ liệu lên các dịch vụ lưu trữ trực tuyến;
- Kiểm soát thiết bị lưu trữ được sử dụng;
- Sau khi hoàn thành công việc phải thực hiện thu hồi, xóa hoặc hủy dữ liệu tạm theo quy định.

Đặc biệt, đối với dữ liệu cá nhân, dữ liệu nghiệp vụ hoặc dữ liệu thuộc phạm vi bảo vệ, cần kiểm soát chặt chẽ việc tiếp cận, sao chép và sử dụng trong quá trình hỗ trợ kỹ thuật.

V. KIỂM SOÁT PHẦN MỀM VÀ THIẾT BỊ ĐƯỢC CÀI ĐẶT

Trong quá trình khắc phục, sửa chữa, đề nghị không sử dụng phần mềm không rõ nguồn gốc, phần mềm bẻ khóa hoặc các công cụ điều khiển từ xa không được kiểm soát. Đối với phần mềm, tiện ích hoặc công cụ kỹ thuật được cài đặt để phục vụ sửa chữa, cần:

- Xác định rõ nguồn gốc;
- Xác định mục đích sử dụng;
- Chỉ cài đặt trong thời gian cần thiết;
- Gỡ bỏ các công cụ không còn nhu cầu sau khi hoàn thành;
- Kiểm tra lại hệ thống sau khi sửa chữa.

VI. THAY ĐỔI MẬT KHẨU VÀ TÀI KHOẢN SAU KHI HOÀN THÀNH

Sau khi hoàn thành việc sửa chữa, nâng cấp hoặc khắc phục hệ thống, thực hiện:

1. Thay đổi mật khẩu các tài khoản quản trị đã được sử dụng trong quá trình sửa chữa.
2. Rà soát toàn bộ tài khoản trên hệ thống, đặc biệt là tài khoản quản trị và tài khoản hỗ trợ kỹ thuật.
3. Khóa hoặc xóa các tài khoản không còn nhu cầu sử dụng.
4. Rà soát các phần mềm điều khiển từ xa, dịch vụ truy cập từ xa và các kết nối được thiết lập trong quá trình sửa chữa.
5. Kiểm tra lại cấu hình hệ thống, thiết bị mạng và các quyền truy cập trước khi đưa hệ thống trở lại hoạt động bình thường.

VII. KIỂM TRA DỮ LIỆU VÀ HỆ THỐNG SAU KHI KHẮC PHỤC

Sau khi hoàn thành việc sửa chữa, cần kiểm tra:

- Dữ liệu có đầy đủ và nguyên vẹn hay không;
- Các phần mềm có hoạt động bình thường hay không;
- Các tài khoản có bị thay đổi hay không;
- Có phát sinh tài khoản mới hay không;
- Có phần mềm, dịch vụ hoặc kết nối bất thường hay không;
- Các thiết bị có kết nối mạng bất thường hay không;
- Các quyền truy cập có đúng với trạng thái trước khi sửa chữa hay không.
- Đối với hệ thống quan trọng, nên thực hiện kiểm tra nhật ký hoạt động trong và sau thời gian sửa chữa để phát hiện các thao tác bất thường.

VIII. XÂY DỰNG QUY TRÌNH KHẮC PHỤC, SỬA CHỮA HỆ THỐNG

Các phòng, đơn vị nghiên cứu xây dựng quy trình thống nhất đối với hoạt động khắc phục, sửa chữa, bảo trì, nâng cấp hệ thống thông tin, trong đó quy định tối thiểu các 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, khắc phục.
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.

UBND xã đề nghị các phòng, đơn vị:

1. Chỉ đạo các bộ phận chuyên môn và quán triệt toàn bộ cán cán bộ, công chức, viên chức thực hiện sao lưu dữ liệu trước khi tiến hành sửa chữa, nâng cấp, thay thế hoặc cài đặt lại hệ thống, thiết bị có khả năng ảnh hưởng đến dữ liệu.
2. Xây dựng quy trình kiểm soát việc sửa chữa, bảo trì, khắc phục hệ thống thông tin, đặc biệt đối với trường hợp có sự tham gia của doanh nghiệp, đơn vị kỹ thuật bên ngoài.

3. Kiểm soát chặt chẽ quyền truy cập của đơn vị kỹ thuật; cấp quyền theo nguyên tắc tối thiểu cần thiết và thu hồi ngay sau khi hoàn thành công việc.

4. Thực hiện thay đổi mật khẩu, rà soát tài khoản, phần mềm và kết nối sau mỗi lần sửa chữa, bảo trì có sự tham gia của bên thứ ba.

5. Duy trì bản sao lưu độc lập đối với dữ liệu quan trọng; định kỳ kiểm tra khả năng khôi phục dữ liệu.

6. 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, cần ưu tiên áp dụng các biện pháp kiểm soát chặt chẽ hơn trong quá trình sửa chữa, bảo trì và hỗ trợ kỹ thuật.

7. Đối với các văn bản, tài liệu thuộc phạm vi bảo vệ bí mật nhà nước, tuyệt đối không thực hiện soạn thảo, lưu trữ, trao đổi hoặc gửi, nhận trên máy tính cá nhân và các thiết bị không bảo đảm yêu cầu an toàn, bảo mật. Việc soạn thảo văn bản mật phải được thực hiện trên máy tính chuyên dùng bảo mật của UBND xã tại Văn phòng HĐND và UBND xã, theo đúng quy định về bảo vệ bí mật nhà nước và bảo đảm an toàn, an ninh thông tin.

8. 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 trong quá trình sửa chữa, cần kịp thời tạm dừng thao tác không cần thiết, bảo toàn hiện trạng và phối hợp với UBND xã và các cơ quan chức năng để kiểm tra, xác minh, xử lý.

Nơi nhận: 

Ký bởi:
Phạm Tiến
Mạnh
Cơ quan:

- Như kính gửi,

- Lưu: VT, VHXXH^{Son}.

TM. ỦY BAN NHÂN DÂN

KT. CHỦ TỊCH

PHÓ CHỦ TỊCH

Ký bởi: ỦY BAN NHÂN DÂN XÃ HIỆP
Cơ quan: ỦY BAN NHÂN DÂN TỈNH
HƯNG YÊN




Đặng Hải Đăng