

**Phụ lục V**  
**Quy trình quản lý an toàn thiết bị đầu cuối**  
(Kèm theo Quyết định số /QĐ-BNV ngày / /2024  
của Bộ trưởng Bộ Nội vụ)

**Bước 1:** Phân loại các thiết bị đầu cuối

- Thiết bị di động;
- Máy chủ;
- Máy trạm;
- Thiết bị mạng;
- Thiết bị lưu trữ.

**Bước 2:** Dán nhãn và đặt tên cho các thiết bị đầu cuối

- Thông tin về thiết bị đầu cuối (Tên, chủng loại, địa chỉ MAC, địa chỉ IP, ngày mua, thời hạn bảo hành);
- Tên máy trạm được đặt theo quy tắc (ví dụ: Văn Sỹ Hùng, Vụ Chính quyền địa phương, phòng 625 thì tên máy tính sẽ được đặt là HungVS\_CQDP\_625);
- Tên máy chủ được đặt theo dịch vụ được cung cấp bởi máy chủ. Ví dụ: máy chủ cung cấp dịch vụ DNS được đặt tên là ServerDNS.

**Bước 3:** Kiểm tra, đánh giá, xử lý điểm yếu an toàn thông tin các thiết bị đầu cuối trước khi đưa vào sử dụng

- Quản lý theo địa chỉ IP, địa chỉ MAC;
- Các thiết bị đầu cuối phải được rà quét điểm yếu về an toàn thông tin trước khi đưa vào sử dụng;
- Các thiết bị di động kết nối mạng không dây được quản lý bằng thiết bị quản lý truy cập mạng không dây tập trung. Người dùng không tự ý lắp đặt các thiết bị phát mạng di động;
- Các máy chủ, máy trạm phải được cài đặt chương trình diệt virus và cập nhật các bản vá cho hệ điều hành, ứng dụng, phần mềm, gỡ bỏ các phần mềm không cần thiết;
- Các thiết bị mạng phải được cấu hình tối ưu cho hệ thống, rà soát các tài khoản quản trị (thay đổi thông tin tài khoản quản trị mặc định, rà soát các tài khoản lạ trên thiết bị, theo dõi lưu lượng bất thường trên thiết bị, cập nhật các bản vá lỗi về an toàn thông tin,...);
- Các thiết bị lưu trữ (USB, ổ cứng di động, SAN, ...) phải được rà soát về an toàn thông tin trước khi sử dụng.

**Bước 4:** Cấp tài khoản cho người sử dụng thiết bị đầu cuối

- Tài khoản quản trị hệ thống phải xác thực 2 lớp hoặc giải pháp quản lý tài khoản đặc quyền;

- Các tài khoản máy chủ, máy trạm, thiết bị mạng được cấp theo tên người sử dụng, phải đặt mật khẩu mạnh cho các tài khoản. Không cấp tài khoản quản trị máy tính cho người dùng;

- Khi truy cập và sử dụng thiết bị đầu cuối từ xa phải có cơ chế xác thực và sử dụng giao thức mạng an toàn.

**Bước 5:** Lưu nhật ký sử dụng (Log)

- Các thiết bị đầu cuối phải được lưu log tập trung ít nhất là 3 tháng;

- Khi xảy ra sự cố các hành vi xoá log, xoá dữ liệu, xoá hệ điều hành, khôi phục hệ thống về trạng thái ban đầu là hành vi cản trở điều tra sự cố an toàn thông tin.

**Bước 6:** Cài đặt, kết nối, gỡ bỏ thiết bị đầu cuối

- Khi cài đặt, kết nối, gỡ bỏ thiết bị đầu cuối phải được sự cho phép của người có thẩm quyền;

- Cài đặt, kết nối thực hiện theo từ Bước 1 đến Bước 5;

- Gỡ bỏ thiết bị đầu cuối ngắt thiết bị ra khỏi hệ thống, xoá hết dữ liệu có trên thiết bị, khôi phục thiết bị về trạng thái ban đầu. Đối với thiết bị mạng khi gỡ bỏ phải đảm bảo trạng thái hoạt động bình thường của hệ thống. Đối với thiết bị phải huỷ bỏ phải đảm bảo khi huỷ bỏ thiết bị không còn sử dụng được, không có khả năng khôi phục được dữ liệu.