**PHỤ LỤC VI**

YÊU CẦU VỀ AN TOÀN THÔNG TIN  
*(Ban hành kèm theo Thông tư số 09/2024/TT-BTNMT ngày 31 tháng 7 năm 2024 của Bộ trưởng Bộ Tài nguyên và Môi trường)*

|  |  |  |
| --- | --- | --- |
| **TT** | **Yêu cầu kỹ thuật** | **Mô tả yêu cầu** |
| **I** | **Xác thực** | |
| 1 | Có chức năng xác thực người sử dụng khi truy cập, quản trị, cấu hình phần mềm. | - Có giao diện quản lý tài khoản người sử dụng.  - Yêu cầu xác thực người sử dụng khi truy cập quản trị, cấu hình phần mềm.  - Yêu cầu xác thực người sử dụng khi truy truy cập sử dụng phần mềm. |
| 2 | Có chức năng cho phép lưu trữ có mã hóa thông tin xác thực hệ thống. | Thông tin xác thực được lưu trữ có mã hóa trên Phần mềm sử dụng thuật toán hash từ SHA-256, SHA-512, SHA-3 và các thuật toán tương đương |
| 3 | Có chức năng cho phép thiết lập chính sách mật khẩu người sử dụng. | - Có chức năng yêu cầu người dùng đặt mật khẩu mới khi đăng nhập lần đầu sử dụng mật khẩu mặc định.  - Có chức năng cho phép thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự.  - Có chức năng cho phép thiết lập thời gian yêu cầu thay đổi mật khẩu.  - Có chức năng cho phép thiết lập thời gian mật khẩu hợp lệ.  - Khóa tài khoản và yêu cầu nhập mật khẩu mới khi mật khẩu của tài khoản đó hết hạn thời gian hợp lệ.  - Mở khóa tài khoản khi thay đổi mật khẩu thành công đối với trường hợp mật khẩu hết hạn thời gian hợp lệ. |
| 4 | Có chức năng cho phép hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất định | - Có giao diện cho phép thiết lập chính sách về giới hạn số lần đăng nhập sai trong khoảng thời gian nhất định.  - Có chức năng cảnh báo tới người sử dụng khi vi phạm chính sách.  - Có chức năng tự động ngăn cản việc đăng nhập tự động khi vi phạm chính sách trên.  - Có chức năng tự động vô hiệu hóa tài khoản nếu vi phạm chính sách trên. |
| 5 | Có chức năng cho phép mã hóa thông tin xác thực trước khi gửi qua môi trường mạng | Chức năng bảo đảm mật khẩu được mã hóa trước khi gửi qua môi trường mạng. |
| 6 | Có chức năng cho phép sử dụng cơ chế xác thực đa nhân tố để xác thực người sử dụng | - Có giao diện cho phép quản trị viên quản lý chính sách về xác thực đa nhân tố.  - Tích hợp các bước xác thực đa nhân tố khi chính sách đối với trường hợp này được kích hoạt. |
| **II** | **Kiểm soát truy cập** | |
| 1 | Có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout). | - Có chức năng cho phép thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi Phần mềm không nhận được yêu cầu từ người dùng.  - Hiển thị thông báo, đóng phiên kết nối đã hết hạn thời gian timeout và yêu cầu đăng nhập lại. |
| 2 | Có chức năng cho phép giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa. | - Có giao diện cho phép quản trị viên quản lý chính sách về giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa.  - Có chức năng thực thi chính sách về giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị Phần mềm từ xa ở trên. |
| 3 | Có chức năng cho phép phân quyền và cấp quyền tối thiểu truy cập, quản trị, sử dụng tài nguyên khác nhau của Phần mềm với người sử dụng/ nhóm người sử dụng có chức năng, yêu cầu nghiệp vụ khác nhau. | - Có giao diện cho phép quản trị viên quản lý chính sách về phân quyền tài khoản theo từng nhóm tài khoản.  - Phân loại nhóm tài khoản theo ít nhất 03 nhóm, gồm: tài khoản người sử dụng thông thường; tài khoản quản trị mức sử dụng; tài khoản quản trị mức phát triển, vận hành.  - Có chức năng thực thi chính sách phân quyền và cấp quyền tối thiểu truy cập, quản trị, sử dụng tài nguyên khác nhau ở trên. |
| 4 | Có chức năng cho phép thiết lập quyền tối thiểu (quyền truy cập, quản trị) cho tài khoản quản trị ứng dụng theo quyền hạn. | - Có giao diện cho phép quản trị viên thiết lập quyền cho các tài khoản.  - Có chức năng thực thi chính sách phân quyền cho các tài khoản ở trên. |
| **III** | **Nhật ký hệ thống** | |
| 1 | Có chức năng cho phép ghi nhật ký hệ thống gồm những thông tin. | - Phần mềm cung cấp chức năng ghi nhật ký hệ thống.  - Nhật ký hệ thống được phân loại theo ít nhất 05 nhóm, gồm: nhật ký truy cập Phần mềm; nhật ký đăng nhập khi quản trị Phần mềm; nhật ký các lỗi pnát sinh trong quá trình hoạt động; nhật ký quản lý tài khoản; nhật ký thay đổi cấu hình Phần mềm. |
| 2 | Có chức năng cho phép quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung. | - Có giao diện cho phép quản trị viên quản lý chính sách về nhật ký hệ thống.  - Cho phép quản trị viên cấu hình khoảng thời gian lưu trữ nhật ký qua giao diện trên.  - Lưu trữ nhật ký với ít nhất 05 thông tin, gồm: thời điểm sinh nhật ký; phân nhóm nhật ký; mô tả thao tác/lỗi; đối tượng thực hiện thao tác/sinh lỗi; mức độ quan trọng. |
| **IV** | **An toàn ứng dụng và mã nguồn** | |
| 1 | Có chức năng cho phép kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý. | Có chức năng thực thi việc kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý. |
| 2 | Có chức năng cho phép bảo vệ ứng dụng chống lại những dạng tấn công phổ biến: SQL Injection, OS command injection, RFI, LFI, Xpath injection, XSS, CSRF | Phần mềm được kiểm tra, đánh giá, kiểm thử xâm nhập theo tiêu chuẩn OWASP và không tồn tại điểm yếu cho phép kẻ tấn công khai thác thông qua các dạng tấn công: SQL Injection, OS command injection, RFI, LFI, Xpath Injection, XSS, CSRF. |
| 3 | Có chức năng cho phép kiểm soát lỗi, thông báo lỗi từ ứng dụng. | - Có chức năng kiểm soát lỗi, chỉ hiển thị các thông báo lỗi được kiểm soát đến người dùng và không hiển thị các lỗi bên trong hệ thống.  - Có chức năng hiển thị thông báo lỗi đến người sử dụng. |
| 4 | Có chức năng cho phép bảo đảm không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng. | Thông tin xác thực, bí mật không được đưa trực tiếp vào mã nguồn ứng dụng mà phải được thiết lập thông qua giao diện cấu hình hệ thống. |
| **V** | **Bảo mật thông tin liên lạc** | |
|  | Có chức năng cho phép mã hóa thông tin, dữ liệu trước khi truyền đưa, trao đổi qua môi trường mạng (đối với các ứng dụng yêu cầu sử dụng chữ ký số). | Có chức năng cho phép mã hóa dữ liệu trước khi truyền đưa, trao đổi qua môi trường mạng sử dụng chữ ký số. |
| **VI** | **Sao lưu dự phòng** | |
| 1 | Có chức năng cho phép tự động sao lưu dự phòng. | - Có giao diện cho phép quản trị viên thiết lập chính sách về sao lưu dự phòng cơ sở dữ liệu và cấu hình hệ thống.  - Có chức năng cho phép thực hiện việc sao lưu dự phòng theo chính sách ở trên. |
| 2 | Có chức năng cho phép phép gán nhãn loại dữ liệu được lưu trữ theo quy tắc được thiết lập. | - Có giao diện cho phép quản trị viên quản lý chính sách về phân loại dữ liệu được lưu trữ theo từng nhóm dữ liệu.  - Có chức năng cho phép lưu trữ dữ liệu theo tên định dạng đối với từng loại dữ liệu tại mục trên. |