BỘ GIAO THÔNG VẬN TẢI

**Hợp đồng**

**Xây dựng hệ thống thông tin Quản lý cán bộ**

**Bộ Giao Thông Vận Tải theo mô hình tập trung**

**TÀI LIỆU**

**HƯỚNG DẪN CÀI ĐẶT VÀ QUẢN TRỊ HỆ THỐNG**

**Phiên bản tài liệu: 1.1**

**Đơn vị quản lý:**

**Đơn vị thực hiện:**

**Hà Nội – …/2022**

**TRANG KÝ**

**Đại diện đơn vị thi công**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Ngày** | **Họ tên** | **Vai trò** | **Ký tên** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |

**Đại diện Tổ Giám sát thi công**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Ngày** | **Họ tên** | **Vai trò** | **Ký tên** |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
| 6 |  |  |  |  |
| 7 |  |  |  |  |
| 8 |  |  |  |  |

**BẢNG GHI NHẬN THAY ĐỔI**

| **Ngày** | **Phiên bản tài liệu** | **A, M, D,**  **R** | **Mô tả** | **Tác giả** |
| --- | --- | --- | --- | --- |
| 25/11/2022 | V1.0 | A | Tạo mới | Vũ Bá Quang |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

*A: Thêm mới; M: Sửa đổi; D: Xóa; R: Rà soát*

MỤC LỤC

[1 TỔNG QUAN TÀI LIỆU 6](#_Toc120269040)

[1.1 Mục đích 6](#_Toc120269041)

[1.2 Thuật ngữ và định nghĩa 6](#_Toc120269042)

[2 QUẢN TRỊ HỆ THỐNG 7](#_Toc120269043)

[2.1 QUẢN TRỊ PHÂN QUYỀN 7](#_Toc120269045)

[2.1.1 Danh mục vai trò – nhóm quyền 7](#_Toc120269046)

[2.1.2 Quản lý người dùng – phân quyền 12](#_Toc120269047)

[3 QUẢN TRỊ VẬN HÀNH MÁY CHỦ 19](#_Toc120269048)

[3.1 Quản trị máy chủ 20](#_Toc120269049)

[3.2 Quản lý nhật ký sự kiện an toàn thông tin – SIEM 20](#_Toc120269050)

[4 BẢO ĐẢM AN TOÀN MÁY CHỦ 21](#_Toc120269051)

[4.1 Xác thực và kiểm soát truy cập máy chủ 21](#_Toc120269052)

[4.2 Cứng hóa máy chủ 22](#_Toc120269053)

[5 BẢO ĐẢM AN TOÀN ỨNG DỤNG 23](#_Toc120269054)

[5.1 Xác thực và kiểm soát truy cập ứng dụng 23](#_Toc120269055)

[5.2 Bảo đảm an toàn dữ liệu 24](#_Toc120269056)

[6 SAO LƯU VÀ PHỤC HỒI DỮ LIỆU 25](#_Toc120269057)

[6.1 Sao lưu 25](#_Toc120269058)

[6.2 Phục hồi dữ liệu 25](#_Toc120269059)

[6.2.1 Tình huống 1: Các DataFile hỏng hoặc mất 25](#_Toc120269060)

[6.2.2 Tình huống 2: Phục hồi các Tablespace 26](#_Toc120269061)

[6.2.3 Tình huống 3: Phục hồi lỗi Control File 26](#_Toc120269062)

[6.2.4 Tình huống 4: Phục hồi lỗi Online Redo LogFile 27](#_Toc120269063)

[6.2.5 Tình huống 5: Phục hồi đến một thời điểm xác định trong quá khứ 27](#_Toc120269064)

[6.2.6 Tình huống 6: Phục hồi đến một System Change Number (SCN) 27](#_Toc120269065)

[6.2.7 Tình huống 7: Phục hồi đến một Sequence log Number 27](#_Toc120269066)

[6.2.8 Phục hồi dữ liệu trong trường hợp hỏng hóc nặng 27](#_Toc120269067)

# TỔNG QUAN TÀI LIỆU

## Mục đích

Mục đích của tài liệu này là hướng dẫn người dùng cách cài đặt và vận hành hệ thống “Phần mềm hệ thống thông tin quản lý cán bộ Bộ Giao Thông Vận Tải"

## Thuật ngữ và định nghĩa

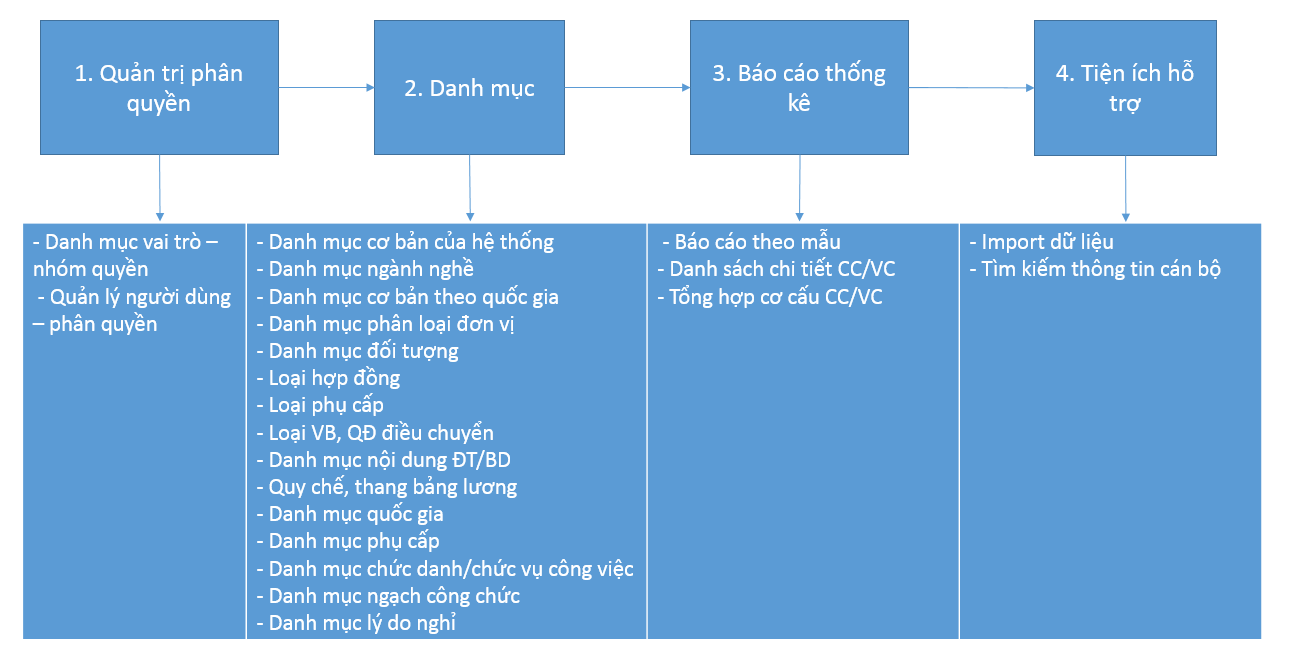
|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Từ viết tắt** | **Từ đầy đủ** | **Mô tả** |
| 1 | CSDL | Cơ sở dữ liệu | Cơ sở dữ liệu mà hệ thống quản lý |
| 2 | NSD | Người sử dụng | Mọi người sử dụng hệ thống |
| 3 | BGTVT | Bộ Giao Thông Vận Tải |  |
| 4 | KBNN | Kho bạc nhà nước |  |
| 5 | HTKT | Hạ tầng kỹ thuật | Phòng Hạ tầng Kỹ thuật |
| 6 | ATTT | An toàn thông tin | Phòng An toàn thông tin |
| 7 | QLCB | Quản lý cán bộ | Phần mềm Quản lý cán bộ |
| 8 | TDKT | Thi đua khen thưởng | Phần mềm Thi đua khen thưởng |
| 9 | AD | Active Directory | Hệ thống quản lý người dùng |
| 10 | API | Application programming interface | Giao diện lập trình ứng dụng |
| 11 | VP | Văn phòng | Văn phòng Bộ Giao Thông Vận tải |
| 12 | WAN | Wide area network | Mạng kết nối diện rộng |
| 13 | VPN | Virtual private network | Mạng kết nối riêng ảo |
| 14 | LAN | Local area network | Mạng kết nối cục bộ |
| 15 | IP | Internet protocal | Kết nối internet |
| 16 | HR | Human resource | Nguồn lực nhân sự |

# QUẢN TRỊ HỆ THỐNG

Hệ thống đảm bảo phân cấp quản lý theo đúng quy định hiện hành (phân quyền quản trị xuống từng đơn vị); có khả năng phân quyền nhập dữ liệu đầu vào, tùy biến, cho phép từng đơn vị có thể thay đổi tham số một cách linh hoạt theo yêu cầu quản lý đặc thù mà không làm thay đổi kiến trúc tổng thể; cho phép chuyển đổi dữ liệu từ excel vào hệ thống theo số lượng lớn; cho phép quản lý lịch sử truy cập hệ thống và lịch sử tác động của người dùng.

Đồng thời, hệ thống cung cấp các báo cáo, thống kê theo yêu cầu người sử dụng; cung cấp các báo cáo tùy biến và chuyên sâu theo yêu cầu; cho phép tra cứu thông tin theo nhiều chiều; cung cấp các công cụ cảnh báo hỗ trợ cán bộ nghiệp vụ…

Bao gồm các nghiệp vụ:



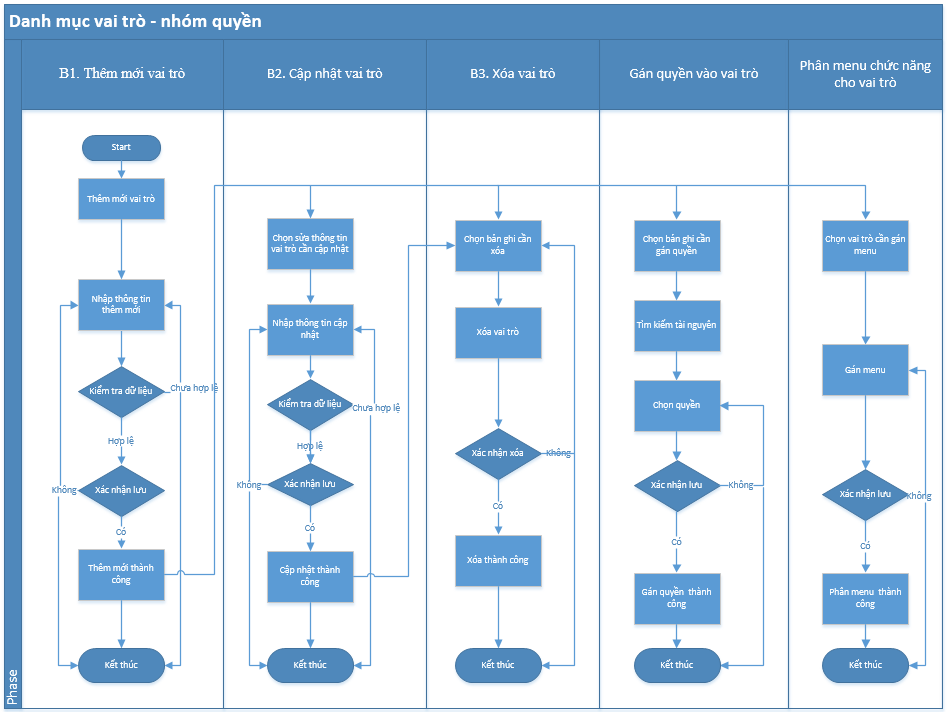


## QUẢN TRỊ PHÂN QUYỀN

### Danh mục vai trò – nhóm quyền

#### **Mô tả**

Danh mục vai trò – nhóm quyền Là module định nghĩa các vai trò sử dụng hệ thống. Cho phép người dùng thiết lập vai trò phù hợp để gán với từng user khác nhau. Mỗi vai trò sẽ có chức năng, quyền hạn khác nhau

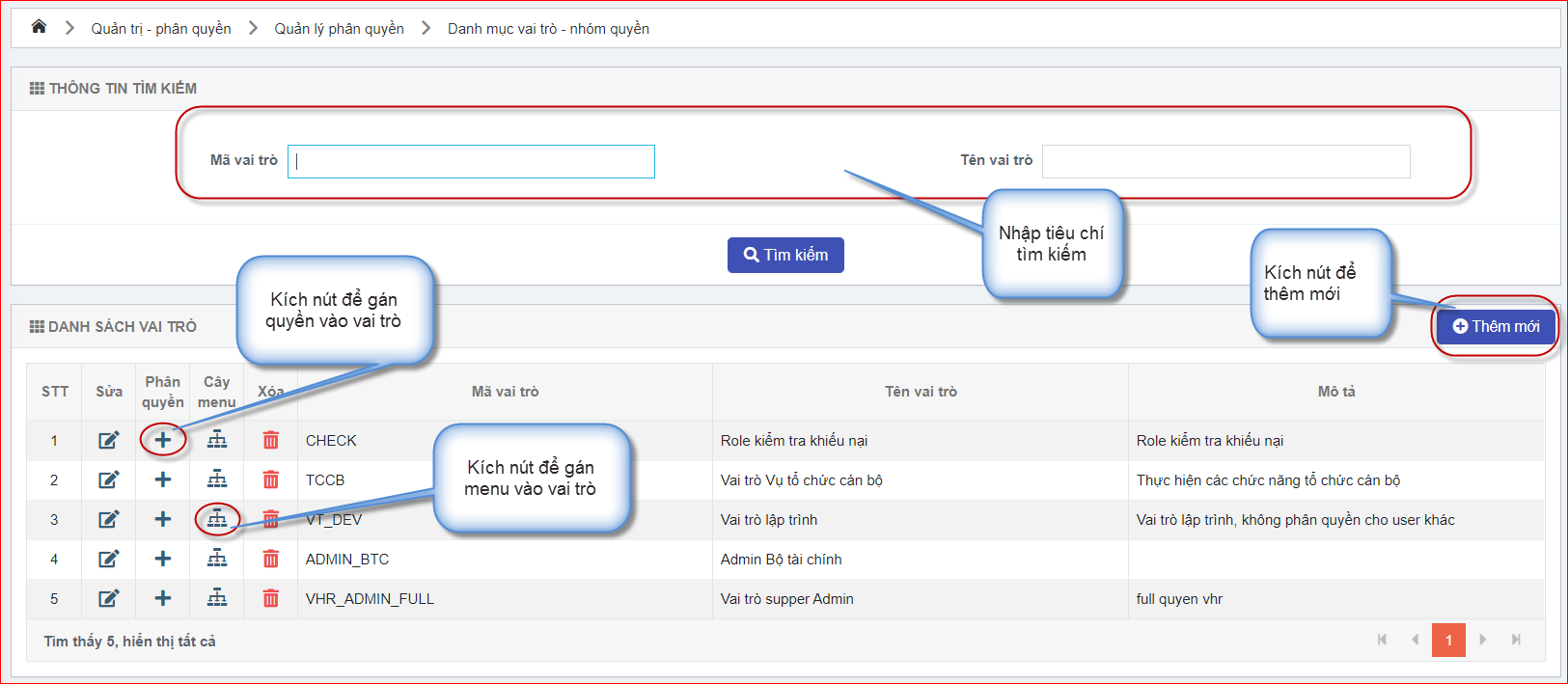


#### **Các thao tác**

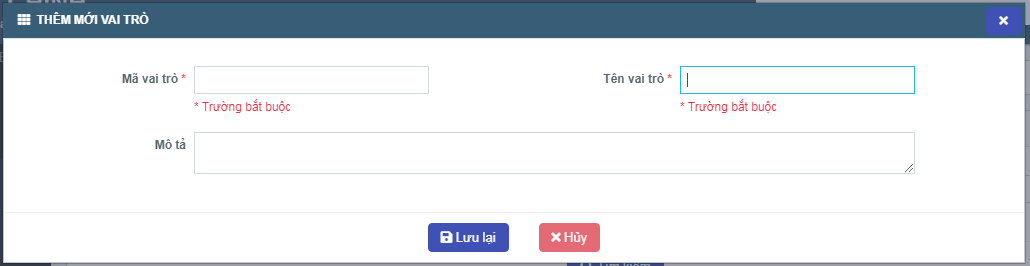
* [Thêm mới vai trò](#_3.1.1.3_Thêm_mới)
* [Cập nhật vai trò](#_Cập_nhật_vai)
* [Xóa vai trò](#_Xóa_vai_trò)
* [Gán quyền vào vai trò](#_3.1.1.5_Gán_quyền): cho phép định nghĩa vai trò được thực hiện chức năng gì trên hệ thống
* [Phân menu chức năng cho vai trò](#_3.1.1.6_Phân_menu): Định nghĩa vai trò được nhìn thấy menu chức năng nào trên hệ thống

#### **Thêm mới vai trò**

**Bước 1:** Vào menu Quản trị phân quyền/ Danh mục vai trò – nhóm quyền, kích nút Thêm mới:



Hệ thống hiển thị giao diện thêm mới vai trò:



**Bước 2:** Nhập thông tin thêm mới vai trò:

* Mã vai trò\*: không được trùng nhau. Bắt buộc nhập
* Tên vai trò\*: tên (dễ nhớ) đặt cho vai trò. Bắt buộc nhập
* Mô tả:

**Bước 3:** Nhấn nút lưu lại và xác nhận để hoàn thành việc thêm mới vai trò

Hệ thống kiểm tra dữ liệu:

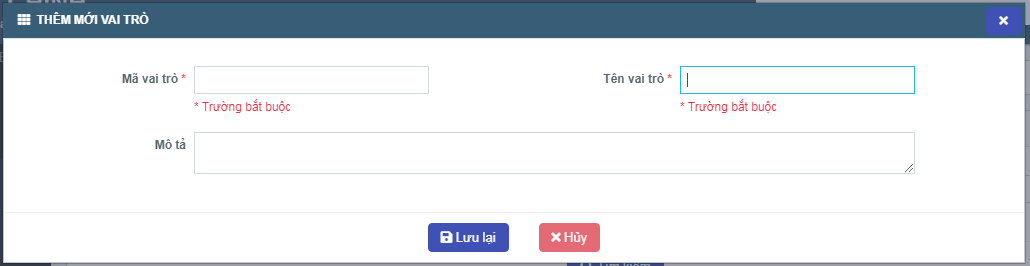
* Nếu dữ liệu nhập lỗi, hệ thống sẽ có các thông báo:
* Nhập trường bắt buộc nếu để trống trường có dấu (\*)
* Các textbox không được nhập ký tự đặc biệt

Người dùng, quay lại **Bước 2** để nhập lại dữ liệu hợp lệ

* Nếu dữ liệu hợp lệ, hệ thống thêm mới thành công:
* Hệ thống có thông báo Lưu dữ liệu thành công
* Bản ghi mới thêm được hiển thị trên giao diện.

#### **Cập nhật vai trò**

**Bước 1:** Tại danh sách các vai trò, chọn vai trò cần thay đổi và kích nút Sửa tương ứng. Hệ thống hiển thị giao diện cập nhật vai trò:



**Bước 2:** Nhập thông tin cần thay đổi:

* Mã vai trò\*: không được trùng nhau. Bắt buộc nhập
* Tên vai trò\*: tên (dễ nhớ) đặt cho vai trò. Bắt buộc nhập
* Mô tả:

**Bước 3:** Nhấn nút lưu lại và xác nhận để hoàn thành việc cập nhật vai trò

Hệ thống kiểm tra dữ liệu:

* Nếu dữ liệu nhập lỗi, hệ thống sẽ có các thông báo:
* Nhập trường bắt buộc nếu để trống trường có dấu (\*)
* Các textbox không được nhập ký tự đặc biệt

Người dùng, quay lại **Bước 2** để nhập lại dữ liệu hợp lệ

* Nếu dữ liệu hợp lệ, hệ thống cập nhật thành công:
* Hệ thống có thông báo Lưu dữ liệu thành công
* Bản ghi mới sửa được hiển thị trên giao diện

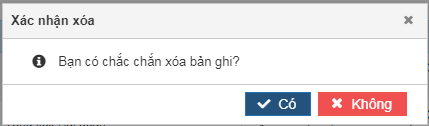
#### **Xóa vai trò**

**Bước 1:** Tại danh sách các vai trò, chọn vai trò cần xóa và kích nút Xóa tương ứng. Hệ thống sẽ kiểm tra ràng buộc:

Nếu vai trò đã được gán cho tài khoản người sử dụng, hệ thống hiển thị thông báo không được phép xóa vai trò

Nếu vai trò chưa được gán cho tài khoản nào, hệ thống hiển thị thông báo xác nhận xóa

Hệ thống hiển thị xác nhận xóa:



**Bước 3:** Xác nhận xóa:

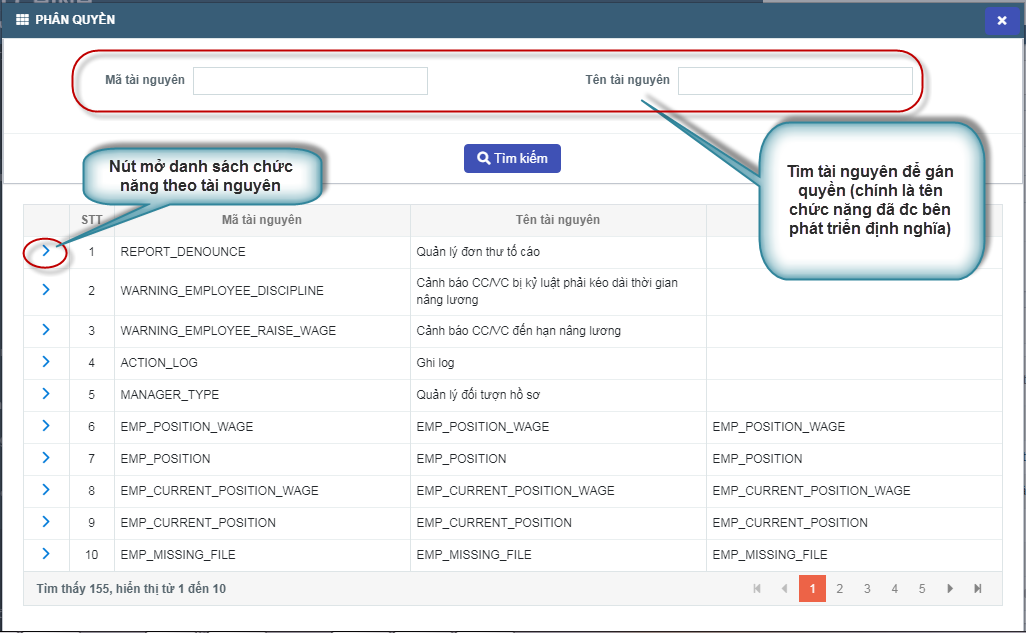
* Nhấn nút Có: đồng ý xóa, hệ thống sẽ xóa hoàn toàn bản ghi.
* Nhấn nút Không: không thực hiện chức năng xóa, hệ thống quay lại màn hình Quản lý vai trò - phân quyền

Nhấn nút Hủy để hủy thao tác xóa. Hệ thống quay lại giao diện Quản lý vai trò – phân quyền mà không thực hiện xóa

#### **Gán quyền vào vai trò**

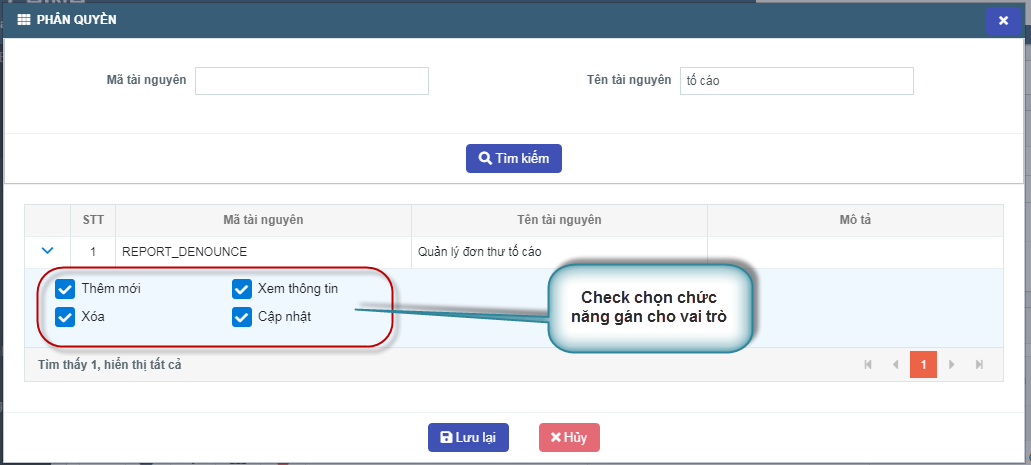
Hệ thống phân quyền đến từng chức năng Thêm/ Sửa/ Xóa/ Xem nên người dùng có thể linh hoạt trong việc phân quyền cho từng vai trò.

**Bước 1**: Tại giao diện Danh mục vai trò – nhóm quyền, chọn Vai trò cần gán quyền và kích nút gán quyền tương ứng:



**Bước 2**: Tìm kiếm chức năng tương ứng được phép sử dụng. Bên phát triển hiển thị Tên tài nguyên tương ứng tên chức năng trên hệ thống

**Bước 3**: Kích nút hiển thị thao tác chức năng được phép sử dụng, và check chọn thao tác gán cho vai trò:

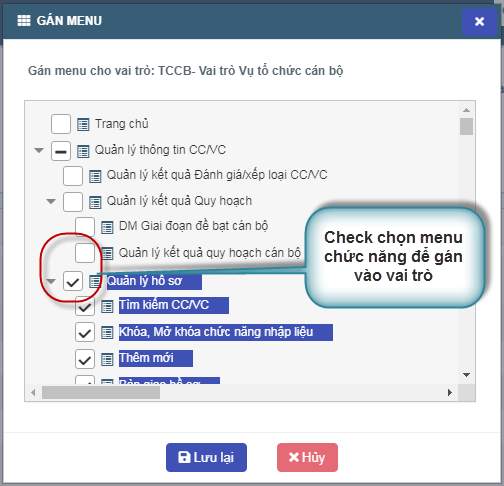


**Bước 4**: Nhấn nút lưu lại và xác nhận để hoàn thành thao tác phân quyền cho Vai trò

#### **Phân menu chức năng cho vai trò**

Với từng vai trò được phân quyền sẽ nhìn thấy menu hệ thống Bộ Giao Thông Vận Tải khác nhau dựa vào chức năng phân menu này.

**Bước 1:** Tại giao diện Danh mục vai trò – nhóm quyền, chọn Vai trò cần gán menu và kích nút gán menu  tương ứng, hệ thống hiển thị cây menu chức năng của hệ thống:

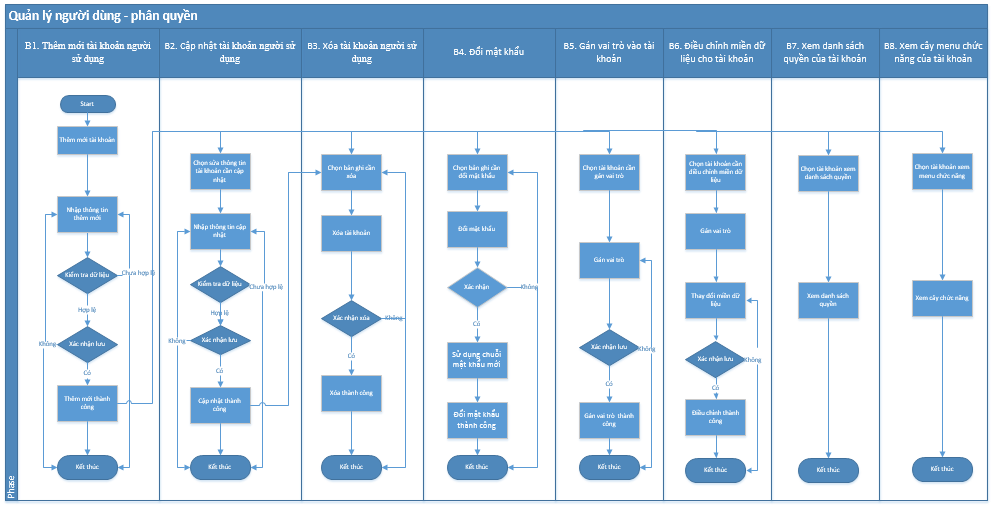


**Bước 2:** Check chọn menu cần gán cho Vai trò

**Bước 3**: Nhấn nút Lưu lại và xác nhận để hoàn thành thao tác phân menu cho Vai trò

### Quản lý người dùng – phân quyền

Là chức năng để thêm/sửa/xóa user có quyền đăng nhập vào hệ thống với từng vai trò tương ứng:

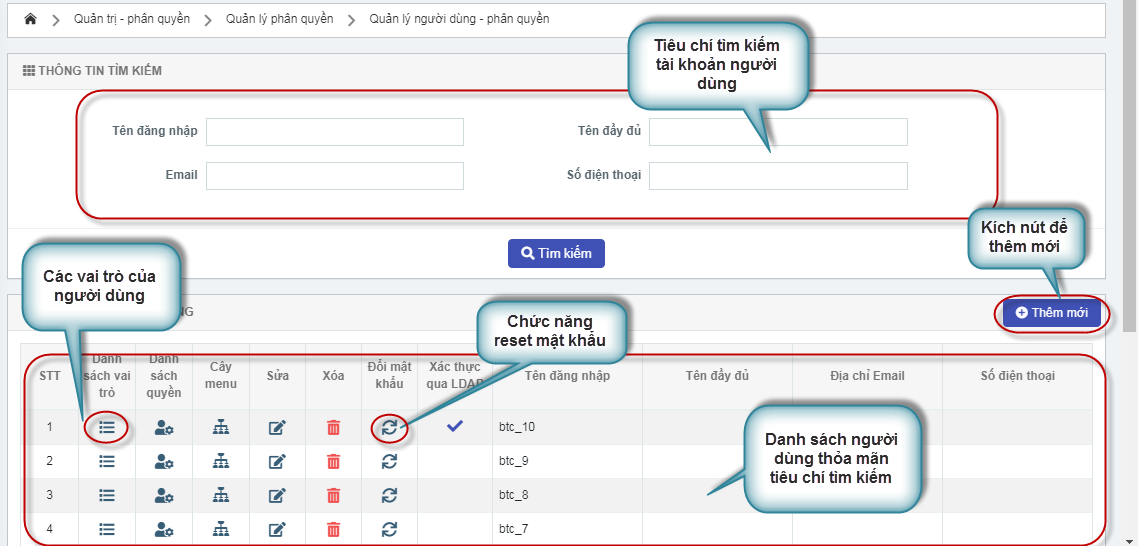


#### **Các thao tác**

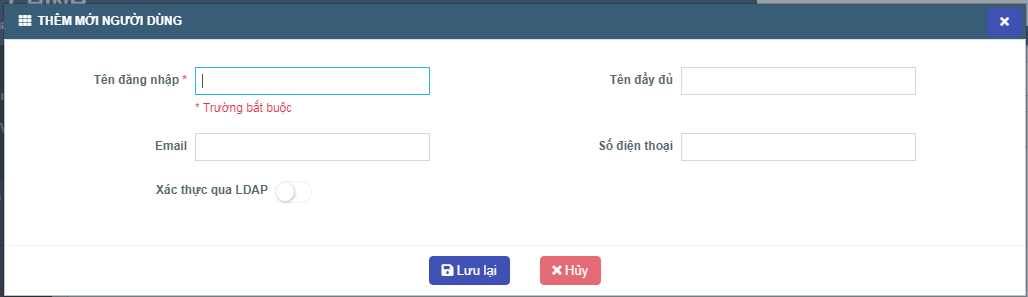
* [Thêm mới tài khoản người sử dụng](#_Thêm_mới_tài)
* [Cập nhật](#_Cập_nhật_tài)
* [Xóa tài khoản người sử dụng](#_Xóa_tài_khoản)
* [Đổi mật khẩu](#_Đổi_mật_khẩu)
* [Gán vai trò vào tài khoản](#_Gán_vai_trò)
* [Điều chỉnh miền dữ liệu cho tài khoản](#_Điều_chỉnh_miền)
* [Xem danh sách quyền](#_Xem_danh_sách)
* [Xem cây menu chức năng](#_Xem_danh_sách_1)

#### **Thêm mới tài khoản người sử dụng**

**Bước 1**: Tại giao diện Quản lý người dùng – phân quyền, kích nút Thêm mới.



Hệ thống hiển thị giao diện thêm mới người sử dụng:



**Bước 2**: Nhập thông tin thêm mới:

* Tên đăng nhập\*: sử dụng để đăng nhập hệ thống. Không được phép trùng nhau
* Tên đầy đủ: Tên sẽ hiển thị trên hệ thống khi đăng nhập thành công
* Email:
* Số điện thoại:
* Xác thực qua LDAP: cho phép đăng nhập hệ thống thông qua tài khoản đăng nhập máy tính. Nếu check chọn thì Tên đăng nhập phải trùng với tên đăng nhập vào máy tính thì mới đăng nhập thành công

**Bước 3**: Nhấn nút Lưu lại để hoàn thành thao tác thêm mới người dung

Hệ thống kiểm tra dữ liệu:

* Nếu dữ liệu nhập lỗi, hệ thống sẽ có các thông báo:
* Nhập trường bắt buộc nếu để trống trường có dấu (\*)
* Các textbox không được nhập ký tự đặc biệt

Người dùng, quay lại **Bước 2** để nhập lại dữ liệu hợp lệ

* Nếu dữ liệu hợp lệ, hệ thống thêm mới thành công:
* Hệ thống có thông báo Lưu dữ liệu thành công
* Bản ghi mới thêm được hiển thị trên giao diện

***Lưu ý:*** *Khi thêm mới thành công, hệ thống không tự sinh mật khẩu để đăng nhập. Người dùng phải dùng chức năng Đổi mật khẩu để lấy mật khẩu đăng nhập*

#### **Cập nhật tài khoản người sử dụng**

**Bước 1**: Tại danh sách tài khoản người sử dụng, chọn bản ghi cần thay đổi và nhấn nút Sửa tương ứng

**Bước 2**: Nhập các thông tin cần thay đổi (tham khảo [Thêm mới người sử dụng](#_Thêm_mới_tài))

**Bước 3**: Nhấn nút Lưu lại và xác nhận để hoàn thành thao tác cập nhật

Hệ thống kiểm tra dữ liệu:

* Nếu dữ liệu nhập lỗi, hệ thống sẽ có các thông báo:
* Nhập trường bắt buộc nếu để trống trường có dấu (\*)
* Các textbox không được nhập ký tự đặc biệt

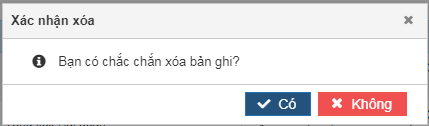
Người dùng, quay lại **Bước 2** để nhập lại dữ liệu hợp lệ

* Nếu dữ liệu hợp lệ, hệ thống cập nhật thành công:
* Hệ thống có thông báo Lưu dữ liệu thành công
* Bản ghi mới sửa được hiển thị trên giao diện

#### Xóa tài khoản người sử dụng

**Bước 1:** Tại danh sách tài khoản người dùng, chọn tài khoản cần xóa và kích nút Xóa tương ứng. Hệ thống kiểm tra ràng buộc:

* Nếu tài khoản đã được gán vai trò, hệ thống hiển thị thông báo không được phép xóa
* Nếu chưa được gán vai trò, hệ thống sẽ hiển thị thông báo xác nhận xóa

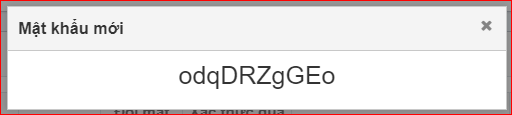


**Bước 2:** Xác nhận xóa:

* Nhấn nút Có: đồng ý xóa, hệ thống sẽ xóa hoàn toàn bản ghi.
* Nhấn nút Không: không thực hiện chức năng xóa, hệ thống quay lại màn hình Quản lý người dùng - phân quyền
* Nhấn nút Hủy để hủy thao tác xóa. Hệ thống quay lại giao diện Quản lý tài khoản người sử dụng mà không thực hiện xóa.

#### **Đổi mật khẩu**

Để thực hiện đổi mật khẩu, người dùng kích nút Đổi mật khẩu tương ứng với tài khoản cần đổi và xác nhận. Hệ thống hiển thị chuỗi mật khẩu mới, ví dụ:

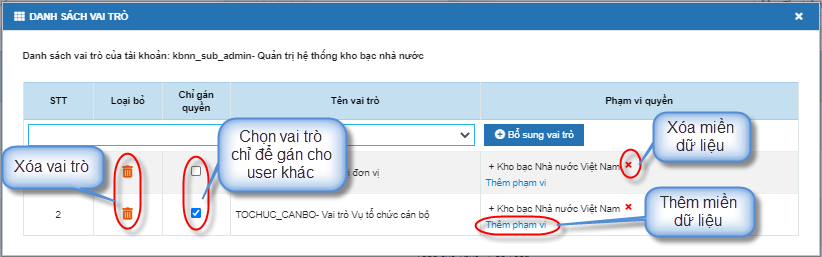


Người dùng sử dụng mật khẩu này để thực hiện đăng nhập hoặc tự đổi sang mật khẩu dễ nhớ ngay trên giao diện đăng nhập hệ thống.

#### **Gán vai trò cho tài khoản người dùng**

Là chức năng hiển thị danh sách vai trò. Đồng thời có thể thêm/sửa/xóa vai trò của người dùng.

**Bước 1**: Tại giao diện Quản lý người dùng – phân quyền, chọn tài khoản cần gán vai trò và kích nút danh sách vai trò  tương ứng:



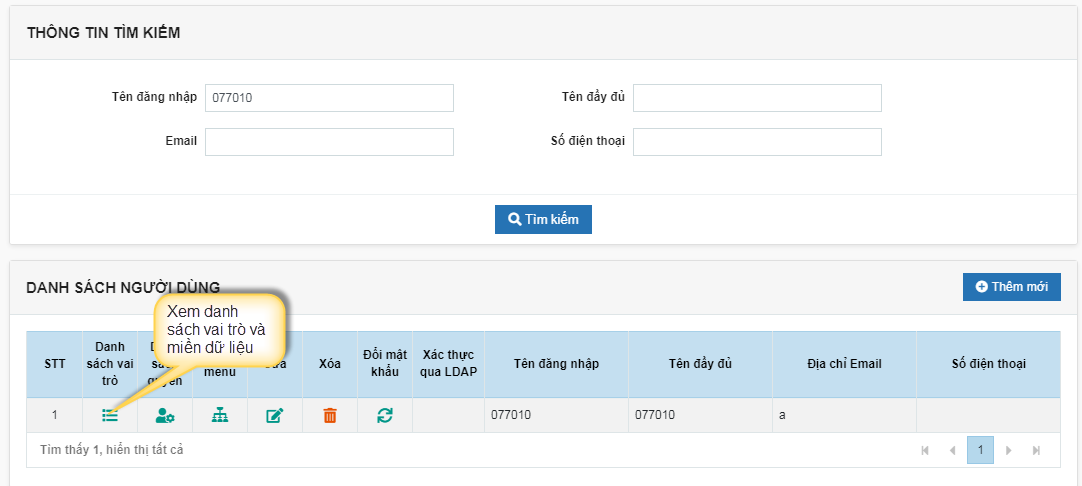
**Bước 2:** Tại giao diện Danh sách vai trò, người dùng có thể thực hiện các chức năng:

* Thêm vai trò cho tài khoản: chọn vai trò trong danh sách và kích nút Bổ sung vai trò. Người dùng là QTHT các đơn vị thuộc Bộ Tài chính chỉ được phép gán các vai trò cho user khác là vai trò đã được gán cho tài khoản của mình.
* Thay đổi miền dữ liệu: bằng cách kích nút Thêm phạm vi để thêm miền dữ liệu, hoặc nút xóa để xóa miền dữ liệu đã được phân
* Xóa vai trò
* Check/Uncheck Chỉ được phân quyền: với các vai trò được check *Chỉ được phân quyền* thì tài khoản được gán chỉ được nhìn thấy vai trò để gán cho user khác mà không có quyền tác động đến các chức năng thuộc vai trò khi thao tác trên phần mềm

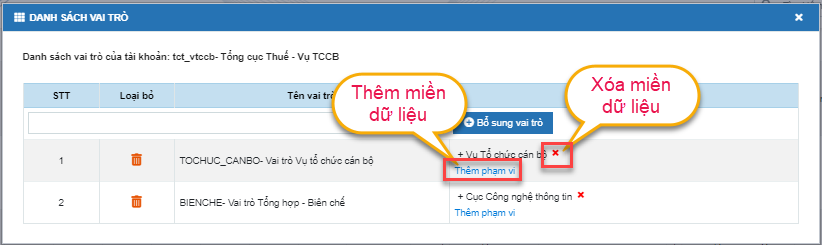
#### **Điều chỉnh miền dữ liệu cho tài khoản người dùng**

Chức năng này hiển thị miền dữ liệu tương ứng của người sử dụng. Đồng thời có thể thêm/sửa/xóa thay đổi miền dữ liệu của người dùng.

**Bước 1**: Tại giao diện Quản lý người dùng – phân quyền, chọn tài khoản cần gán vai trò và kích nút danh sách vai trò  tương ứng:

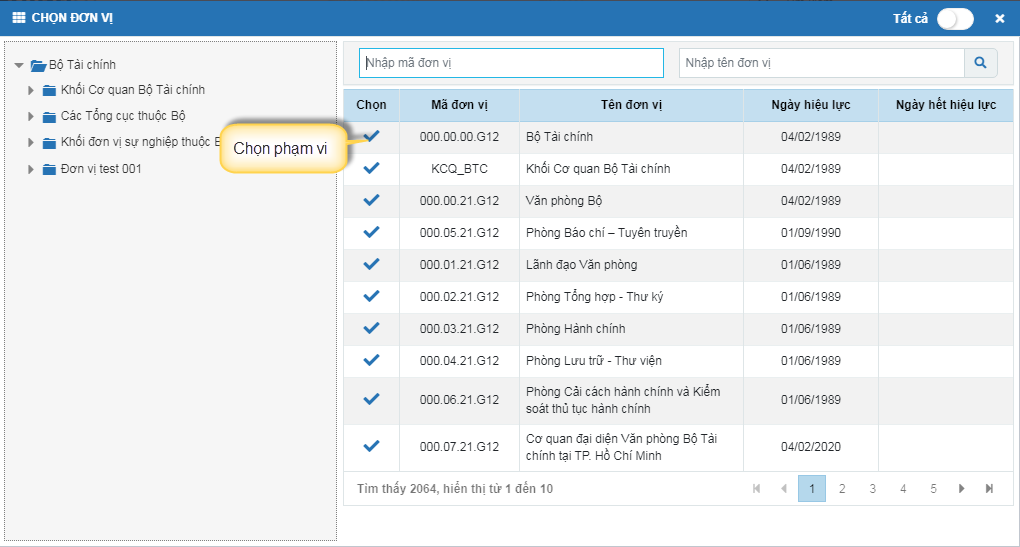


**Bước 2:** Thêm/ Sửa/ Xóa Miền dữ liệu



Các chức năng thêm/ sửa/ xóa miền dữ liệu:

* Xóa miền dữ liệu: bằng cách nhấn vào icon xóa miền dữ liệu đã có như mô tả trong hình
* Để sửa miền dữ liệu: người dùng thực hiện xóa miền dữ liệu hiện có và thêm miền dữ liệu mới
* Thêm miền dữ liệu: người dùng nhấn vào link “Thêm phạm vi” thì hệ thống mở popup chọn phạm vi (là cây đơn vị như hình mô tả dưới). Người dùng có thể nhập tiêu chí để tìm kiếm đơn vị trong phạm vi quản lý của mình, sau đó nhấn “Chọn”, để gán miền dữ liệu cho vai trò tương ứng.



#### **Xem danh sách quyền của tài khoản người sử dụng**

Với các vai trò đã được gán cho tài khoản, người dùng có thể xem danh sách các quyền thuộc tài khoản được phân, bằng cách:

Tại giao diện Quản lý người dùng – phân quyền, kích nút Danh sách quyền  tương ứng tài khoản cần xem:



Người dùng có thể tìm kiếm theo Mã quyền, Tên quyền để lọc danh sách quyền thuộc tài khoản!

#### **Xem cây menu chức năng của tài khoản người sử dụng**

Với các vai trò đã được gán cho tài khoản, người dùng có thể xem danh sách các quyền thuộc tài khoản được phân, bằng cách:

Tại giao diện Quản lý người dùng – phân quyền, kích nút Danh sách quyền  tương ứng tài khoản cần xem:



Người dùng có thể tìm kiếm theo Mã quyền, Tên quyền để lọc danh sách quyền thuộc tài khoản!

# QUẢN TRỊ VẬN HÀNH MÁY CHỦ

## Quản trị máy chủ

* Các máy chủ được kích hoạt và hoạt động ở chế độ tường lửa.
* Máy chủ do phòng HTKT quản lý và vận hành.
* Máy chủ chỉ có thể kết nối trực tiếp từ các máy chủ trung gian tại Bộ Giao Thông Vận Tải.
* Máy chủ cần được kết nối đến hệ thống quản lý nhật ký và sự kiện an toàn thông tin (Security Information and Event Management - SIEM) của Bộ Tài chính.
* Máy chủ cần được đồng bộ về thời gian với máy chủ thời gian (TimeServer) của Bộ Tài chính.
* Trong trường hợp cần thiết (như cài đặt, nâng cấp phần mềm, khắc phục sự cố), đơn vị thi công có thể truy cập và quản trị máy thông qua máy chủ trung gian, dưới sự giám sát và hỗ trợ của cán bộ phòng HTKT.

## Quản lý nhật ký sự kiện an toàn thông tin – SIEM

* Hệ thống có nhiệm vụ giám sát an toàn thông tin tại Bộ Giao Thông Vận Tải bằng các biện pháp sau: Phân tích thông tin trên hệ thống Quản lý nhật ký và sự kiện an ninh (SIEM); Phân tích các sự cố, sự kiện, cảnh báo, báo cáo trên các hệ thống an toàn thông tin mạng.
* Các hệ thống giám sát phải được kiểm tra hàng ngày, đảm bảo hoạt động liên tục 2 Đối tượng giám sát bao gồm: Tất cả các máy chủ, ứng dụng tại Bộ Tài chính; Các thiết bị mạng (switch, router); Các hệ thống kỹ thuật bảo đảm an toàn thông tin mạng.
* Các đối tượng giám sát, loại giám sát phải được kết nối và gửi nhật ký hệ thống tới tới SIEM bao gồm:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TT** | **Đối tượng kết nối SIEM** | | **Loại Log** | **Phương thức** |
| 1 | App  Servers | Tomcat |  | Syslog |
| 3 |  | Máy chủ Database Oracle | Listener Log, Database Log | Agent |
| Oracle RAC | Listener Log, Database Log, Event Manager Log. | SCP |
| Oracle RAC | Audit log | Agent |

* Truy cập và quản trị hệ thống giám sát:
  + Bộ phận quản trị hệ thống quản trị hệ thống giám sát.
  + Bộ phận giám sát an toàn thông tin truy cập hệ thống giám sát để đọc thông tin, phân tích cảnh báo.
  + Phân công cụ thể các cá nhân chịu trách nhiệm quản trị và truy cập sử dụng hệ thống giám sát.
  + Hoạt động quản trị hệ thống giám sát phải được thực hiện từ vùng mạng dành riêng cho công tác quản trị.
  + Truy cập sử dụng hệ thống giám sát chỉ được thực hiện từ vùng mạng dành riêng cho hoạt động quản trị
* Thời gian lưu trữ nhật ký hệ thống: Security Devices, Vcenter: 6 tháng; Network Devices, Servers, Web Server, Applications, Databases: 03 tháng. Trường hợp hệ thống giám sát không đủ dung lượng để đảm bảo thời gian lưu trữ, thực hiện sao lưu thông tin của hệ thống giám sát vào hệ thống lưu trữ tập trung của Bộ Giao Thông Vận Tải, đảm bảo tổng thời gian lưu trữ nhật ký theo quy định. Quản trị hệ thống và người giám sát không được phép xóa thông tin giám sát trên hệ thống giám sát trừ trường hợp phát sinh lỗi tràn ổ cứng
* Đồng bộ thời gian giữa hệ thống giám sát và thiết bị được giám sát: Các hệ thống giám sát và đối tượng giám sát phải đồng bộ thời gian với máy chủ thời gian (TimeServer)
* Đối với hệ thống cấp độ 3, bộ phận giám sát an toàn thông tin thực hiện truy cập, sử dụng thông tin trên hệ thống giám sát để theo dõi, giám sát và cảnh báo sự cố phát hiện trên hệ thống thông tin, phân tích, đưa ra hướng dẫn xử lý và giám sát xử lý trong thời gian làm việc.

# BẢO ĐẢM AN TOÀN MÁY CHỦ

## Xác thực và kiểm soát truy cập máy chủ

* Các máy chủ được đặt trong vùng riêng biệt. Máy chủ CSDL được đặt trong vùng Internal 0.x. Máy chủ ứng dụng được đặt trong vùng 246.x. Việc truy cập chỉ có thể thực hiện thông qua các máy chủ trung gian tại Bộ Giao Thông Vận Tải.
* Mỗi phòng ban trong trung tâm Dữ liệu hạ tầng có thể được cấp tài khoản riêng tùy theo yêu cầu của các phòng ban liên quan, với quyền hạn tương xứng. Định kỳ 02 tuần/ lần sẽ tiến hành rà soát các tài khoản đã cấp, đưa danh sách các tài khoản đã dừng hoạt động hoặc một thời gian dài không thấy truy cập vào hệ thống để lên danh sách tài khoản cần vô hiệu hóa hoặc hủy.
* Mật khẩu xác thực phải thỏa mãn những tiêu chí sau:
  + Với mật khẩu mặc đinh, khi lần đầu tiên người dùng truy cập vào hệ thống sẽ gửi yêu cầu và bắt buộc phải thay đổi mật khẩu này mới được truy cập.
  + Mật khẩu có chiều dài tối thiểu là 8, phải bao gồm chữ cái thường, chữ cái viết hoa, chữ số và ký tự không phải chữ cái hay chữ số. Mật khẩu không được chứa tên tài khoản
  + Thời gian mặc định yêu cầu thay đổi mật khẩu (mặc định 90 ngày và cán bộ quản trị hệ thống có thể thay đổi thông số này) sau thời gian này sẽ yêu cầu người dùng thay đổi mật khẩu.
  + Mật khẩu mới không được trùng với mật khẩu cũ
* Tài khoản đăng nhập sai 5 lần liên tiếp sẽ bị khóa tạm thời 15 phút, không thể đăng nhập trong khoảng thời gian này.
* Quản trị viên có thể thiết lập, thay đổi số lần đăng nhập sai cũng như thời gian vô hiệu hóa tài khoản tạm thời.
* Hệ thống sẽ tự động logout nếu không nhận được yêu cầu từ người dùng sau 30 phút
* Máy chủ phải được đồng bộ với máy chủ thời gian (TimeServer).
* Máy chủ phải được ghi nhật ký đồng bộ lên hệ thống Quản lý nhật ký sự kiện an toàn thông tin (SIEM) như đã nêu ở mục 5.2. Giới hạn 100MB dung lượng để lưu trữ nhật ký hệ thống, tránh mất mát hoặc tràn bộ nhớ. Nhật ký phải được lưu trữ tối thiểu 03 tháng.

## Cứng hóa máy chủ

Để đảm bảo an toàn bảo mật cho máy chủ, cần tiến hành cứng hóa máy chủ trước khi đưa vào vận hành, khai thác theo các tiêu chí sau:

* Máy chủ phải được cập nhật các bản vá lỗi thường xuyên. Đối với máy chủ cài Windows Server, phải được kết nối với hệ thống WSUS của Bộ Giao Thông Vận Tải.
* Máy chủ phải được cài đặt Firewall, phần mềm phòng chống độc hại McAfee theo tiêu chuẩn của Bộ Giao ThôngVận Tải. Phần mềm phòng chống độc hại McAfee được quản lý tập trung, tự cập nhật phiên bản mới, đồng thời đồng bộ nhật ký lên hệ thống SIEM của Bộ Giao Thông Vận Tải như đã nêu trên mục 5.2. Phần mềm phòng chống mã độc McAfee phải được thiết lập cơ chế real-time scan, đảm bảo cho toàn bộ máy chủ luôn được quét liên tục, bất kỳ phần mềm nào trên máy chủ cũng được kiểm tra, quét trước khi cài đặt.
* Các phần mềm cài đặt trên máy chủ phải có bản quyền hoặc nguồn gốc rõ ràng.
* Máy chủ cần được tiến hành cứng hóa theo yêu cầu của phòng ATTT, phải đảm bảo vượt qua công cụ quét bảo mật máy chủ chuyên dụng của Giao ThôngVận Tải.
* Đảm bảo máy chủ đạt tiêu chuẩn bảo mật cấp độ 3 theo tiêu chuẩn TCVN: 11930:2017

# BẢO ĐẢM AN TOÀN ỨNG DỤNG

## Xác thực và kiểm soát truy cập ứng dụng

* Ứng dụng xây dựng trên nền tảng web service, sử dụng tên đăng nhập và mật khẩu để tạo ra các khóa xác thực JWT
  + Việc truyền tải dữ liệu trên dường truyền khi cần xác thực sẽ xử dụng chuỗi JWT để mã hóa/ và giải mã khi truyền/ nhận thông tin giữa trình duyệt web và máy chủ.
  + Các khóa bảo mật JWT được hệ thống sinh và thay đổi thưởng xuyên trong quá trình làm việc
* Các tài khoản trên ứng dụng phải thỏa mãn các tiêu chí sau:
  + Tài khoản được cấp mật khẩu mặc định sẽ bắt buộc phải thay đổi mật khẩu trong lần truy cập ứng dụng đầu tiên
  + Mật khẩu phải tuân thủ quy tắc: có chiều dài tối thiểu là 8, phải bao gồm chữ cái thường, chữ cái viết hoa, chữ số và ký tự không phải chữ cái hay chữ số. Mật khẩu không được chứa tên tài khoản
  + Thời gian mặc định yêu cầu thay đổi mật khẩu (mặc định 90 ngày và cán bộ quản trị hệ thống có thể thay đổi thông số này) sau thời gian này sẽ yêu cầu người dùng thay đổi mật khẩu.
  + Mật khẩu mới không được trùng với mật khẩu cũ
  + Tài khoản đăng nhập sai quá 5 lần sẽ bị khóa tạm thời trong 15 phút. Không thể tiếp tục đăng nhập
* Hệ thống sẽ tự động logout nếu không nhận được yêu cầu từ người dùng sau 30 phút.
* Hệ thống được cấu hình để ngăn cản việc truy cập tự động, khi người sử dụng truy cập sai, hệ thông sẽ sinh mã Capcha để yêu cầu xác thực.
* Hệ thống được cấu hình để phát hiện một tài khoản có nhiều hơn một phiên đăng nhập, hệ thống sẽ sinh ra cảnh báo cho phiên đăng nhập.
* Hệ thống phân quyền chức năng theo vai trò của nhóm người sử dụng. Mỗi người sử dụng sẽ được gán cho một hoặc nhiều vai trò, với các quyền hạn khác nhau (quyền quản trị, quyền nghiệp vụ, quyền khai thác dữ liệu …)
* Mọi thao tác của người dùng trên hệ thống đều được lưu lại:
  + Thông tin tài khoản truy cập đã thao tác
  + Đã thao tác trên chức năng nào, dữ liệu nào đã được thao tác, hành động cụ thể là gì, dữ liệu trước và sau hành động đó; Bao gồm cả dữ liệu nghiệp vụ và thông tin cấu hình sử dụng
  + Các lỗi phát sinh trong quá trình vận hành đều được thông báo cho người dùng ở dạng cảnh báo với nội dung phù hợp, tránh các thông báo sâu về mã nguồn, cơ sở dữ liệu ... ngoài ra các lỗi này cũng được lưu vào trong nhật ký hoạt động của hệ thống
  + Nhật ký được lưu trong khoảng thời gian tối thiểu là 03 tháng. Quản trị viên có thể thay đổi thời gian này.
  + Nhật ký phải được đồng bộ lên hệ thống Quản lý tập trung (SIEM) như đã nêu trên mục 2.5

## Bảo đảm an toàn dữ liệu

* Ứng dụng chỉ cho phép truy cập qua giao thức HTTPS, đảm bảo dữ liệu không bị rò rỉ khi gửi qua môi trường mạng. Chứng thư số được sử dụng được cung cấp bởi nhà cung cấp uy tín GlobalSign theo tiêu chuẩn của Bộ Tài chính.
* Dữ liệu được nhập vào hệ thống sẽ được kiểm tra ở 03 bước:
  + Trên trình duyệt web: dữ liệu được kiểm tra định dạng, tính hợp lệ và cảnh báo ngay mà không cần đợi lệnh gọi về máy chủ
  + Khi dữ liệu được gửi lên máy chủ, để tránh các trường hợp tấn công, hệ thống kiểm tra và xác thực lại dữ liệu
  + Trước khi dữ liệu dược lưu vào Cơ sở dữ liệu hay mang vào các lệnh tính toán, hệ thống thao tác với Cơ sở dữ liệu sẽ kiểm tra dữ liệu một lần nữa; Những dữ liệu không hợp lệ sẽ bị hủy và gửi thông báo cho người dùng cũng như ghi nhật ký thao tác
* Dữ liệu trước khi được xuất ra theo yêu cầu sẽ được rà quét và có hàm kiểm tra loại bỏ những lỗi liên quan đến dữ liệu đầu ra tại tầng nghiệp vụ ứng dụng trươc khi xuống tầng hiển thị.
* Hệ thống phải đảm bảo vượt qua công cụ quét bảo mật ứng dụng chuyên dụng của Bộ Tài chính, đảm bảo thỏa mãn tiêu chuẩn bảo mật cấp độ 3 TCVN: 11930-2017
* Hệ thống phải thực hiện việc lưu log các lỗi xảy ra trong quá trình sử dụng, phục vụ cho việc rà soát và sửa lỗi. Thông báo lỗi thân thiện cho người dùng, không hiển thị cụ thể chi tiết lỗi để đảm bảo an toàn bảo mật.
* Hệ thống sử dụng CSDL Oracle 12c, được lưu trên SAN, đảm bảo tính toàn vẹn của dữ liệu

# SAO LƯU VÀ PHỤC HỒI DỮ LIỆU

## Sao lưu

Sử dụng công cụ chuyên dụng của Bộ Giao ThôngVận Tải để thực hiện sao lưu định kỳ đối với cả máy chủ ứng dụng và CSDL, theo cơ chế như sau:

* Hàng ngày thực hiện sao lưu những thay đổi
* Mỗi tuần thực hiện sao lưu full một lần
* Các bản sao lưu được lưu trữ tối thiểu 01 tháng

## Phục hồi dữ liệu

* Trong quá trình vận hành, một số tình huống gây sự cố cho hệ thống có thể xảy ra như cháy, nổ, hỏng thiết bị phần cứng, lỗi thiết bị lưu trữ… Điều này là không thể tránh khỏi. Các sự cố cũng rất đa dạng, từ hỏng 1 số file quan trọng đến hỏng toàn bộ cơ sở dữ liệu. Tuỳ theo chiến lược sao lưu mà ta có phương án phục hồi tương ứng.
* Đối với máy chủ ứng dụng, chỉ cần restore lại các bản backup bằng công cụ chuyên dụng.
* Đối với CSDL, ta có một số trường hợp sự cố phổ biến nhất và cách khắc phục như sau

### Tình huống 1: Các DataFile hỏng hoặc mất

* Điều kiện: Database instance vẫn còn hoạt động. Các Control File không hỏng và phải có bản Full\_backup
* Cách khắc phục
  + Bước 1: Khởi động Database
  + Bước 2: Tạo tác vụ Phục hồi dữ liệu
  + Bước 3. Chọn nhiệm vụ cho tác vụ
  + Bước 4: Chọn đối tượng để Phục hồi dữ liệu
  + Bước 5: Chọn thời điểm phục hồi gần nhất
  + Bước 6: Kết thúc nhập tham số cho tác vụ Phục hồi
  + Bước 7: Thực hiện Phục hồi dữ liệu
  + Bước 8: Theo dõi quá trình thực hiện tác vụ

### Tình huống 2: Phục hồi các Tablespace

* Một vài tablespace của CSDL hỏng hoặc mất
* Điều kiện: Database instance vẫn start được và có bản Sao lưu Full CSDL
* Cách khắc phục :
  + Bước 1. Tạo tác vụ Khôi phục
  + Bước 2: Chọn nhiệm vụ cho tác vụ
  + Buớc 3: Nhập các thông số cho tác vụ
  + Bước 4: Chọn tablspace cần được restore và Recover
  + Bước 5: Kết thúc nhập tham số và thực hiện
  + Bước 6: theo dõi quá trình thực hiện: Vào phần Job 🡺 Active Job 🡺 History để xem chi tiết tình trạng và quá trình Restore và Recover.

### Tình huống 3: Phục hồi lỗi Control File

* Tình huống mất 1 Control File trong các Control được Mutilplex
* Cách khắc phục:
  + Tạo lại File hỏng từ File không bị hỏng sử dụng lệnh Copy của hệ điều hành và sửa tên ControlFile.
* Tình huống mất toàn bộ Control File của Database
* Điều kiện: Configure backup Control File
* Cách khắc phục : Sử dụng Oracle Enterprise Manager
  + Bước 1: Restore ControlFile
    - Tạo tác vụ Restore ControlFile
    - Nhập các thông tin về việc Restore Control File
    - Thực hiện Restore Controlf File
    - Theo dõi tình trạng Restore
  + Bước 2: Open database ở chế độ Resetlogs.

### Tình huống 4: Phục hồi lỗi Online Redo LogFile

* Tình huống mất 1 Redo LogFile
* Cách khắc phục:
  + Xác định Redo LogFile có phải là tình trạng Active hay không?
  + Nếu là tình trạng Active hoặc Current thì phải
    - SQL> Shutdown abort;
    - SQL> Recover database Until Cancel;
    - SQL> Alter database open resetlogs;
    - Và thực hiện Reset Database vào Catalog;
  + Nếu ngược lại thì chỉ cần tạo lại từ 1 file đã có sử dụng lệnh Copy của hệ điều hành.

### Tình huống 5: Phục hồi đến một thời điểm xác định trong quá khứ

* Bước 1: Tạo tác vụ phục hồi dữ liệu
* Bước 2: Chọn nhiệm vụ thực hiện
* Bước 3: Cập nhật các thông số cho tác vụ
* Bước 4: Kết thúc cập nhật thông tin và thực hiện
* Bước 5: Theo dõi tiến trình thực hiện tác vụ

### Tình huống 6: Phục hồi đến một System Change Number (SCN)

* Các bước thực hiện đều giống với Phần Phục hồi đến một thời điểm xác định trong quá khử chỉ khác là xác đinh số SCN để thực hiện Restore và Recover.

### Tình huống 7: Phục hồi đến một Sequence log Number

* Các bước thực hiện đều giống với Phần Phục hồi đến một thời điểm xác định trong quá khứ chỉ khác là xác định số Sequence và Thread# để thực hiện Restore và Recover.

### Phục hồi dữ liệu trong trường hợp hỏng hóc nặng

* Điều kiện: phải có bản Backup Full và Database phải Start ở chế độ Nomount.

Cách khắc phục: Sử dụng Oracle Enterprise Manager

* + Bước 1: Restore ControlFile
  + Bước 2: Restore và Recover Database
  + Bước 3:
    - SQL> shutdown immediate;
    - SQL> startup mount;
    - SQL> Alter database open resetlogs;
    - SQL> exitl;
    - RMAN> Reset Database.
* Tình huống 2: Mất toàn bộ Redo LogFile

Cách khắc phục:

* + SQL>Shutdown abort;
  + SQL> Startup;
  + Tìm xem thông tin của Logfile để xác định Redo Logfile nào là Current.
  + Các File khác không phải là Current thì thực hiện lệnh:
  + SQL> Alter database clear logfile group <number>;
  + Ra ngoài hệ điều hành tạo lại Current Redo Logfile từ File đã có.
  + SQL> Recover database until Cancel;
  + SQL> Alter database Open Resetlogs;
  + SQL> Shutdown immediate;
  + SQL> Startup
  + Và thực hiện Reset Database vào Catalog;