ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN



ĐỒ ÁN MÔN HỌC

**AN TOÀN BẢO MẬT HTTT ⏐ 2021**

CHỦ ĐỀ: QUẢN LÝ BỆNH VIỆN

CQ2018/1 – NHÓM 10

GVHD: TS. Phạm Thị Bạch Huệ Người thực hiện:

Ths. Lương Vĩ Minh 18120518 – Phạm Thị Bích Phượng

18120538 – Võ Nguyễn Hồng Sơn

18120580 – Đinh Quang Thọ

TP Hồ Chí Minh, ngày 5 tháng 7 năm 2021

NHẬN XÉT CỦA GIÁO VIÊN

Tp. Hồ Chí Minh, ngày … tháng … năm 2019

Giáo viên lý thuyết

NHẬN XÉT CỦA GIẢNG VIÊN

Tp. Hồ Chí Minh, ngày … tháng … năm 2020

Giảng viên hướng dẫn

**MỤC LỤC**

[1. THÔNG TIN NHÓM 4](#_Toc76331081)

[2. BẢNG PHÂN CÔNG CÔNG VIỆC VÀ ĐÁNH GIÁ 4](#_Toc76331082)

[3. MÔ TẢ ĐỒ ÁN CUỐI KỲ 5](#_Toc76331083)

[4. KẾT QUẢ 5](#_Toc76331084)

[4.1. Phân hệ 1 – Hệ thống dành cho người quản trị cơ sở dữ liệu 5](#_Toc76331085)

[**4.1.1.** **Bảng danh sách các yêu cầu đã thực hiện:** 6](#_Toc76331086)

[**4.1.2.** **Giao diện dành cho người quản trị hệ cơ sở dữ liệu** 6](#_Toc76331087)

[4.2. Phân hệ 2 – Quản lý thông tin của một bệnh viện 13](#_Toc76331088)

[**4.2.1.** **Lược đồ cơ sở dữ liệu** 13](#_Toc76331089)

[**4.2.2.** **Các chính sách bảo mật** 14](#_Toc76331090)

[I. Cơ chế DAC, RBAC, VPD 17](#_Toc76331091)

[II. Cơ chế MAC (OLS) 34](#_Toc76331092)

[III. Mã hóa 37](#_Toc76331093)

[IV. Audit 41](#_Toc76331094)

# THÔNG TIN NHÓM

|  |  |  |
| --- | --- | --- |
| MSSV | HỌ TÊN | EMAIL |
| 18120518 | Phạm Thị Bích Phượng | 18120518@student.hcmus.edu.com |
| 18120538 | **Võ Nguyễn Hồng Sơn (\*)** | 18120538@student.hcmus.edu.com |
| 18120580 | Đinh Quang Thọ | 18120580@student.hcmus.edu.com |

(\*): Nhóm trưởng

# BẢNG PHÂN CÔNG CÔNG VIỆC VÀ ĐÁNH GIÁ

|  |  |  |  |
| --- | --- | --- | --- |
| **Người thực hiện** | **Công việc thực hiện** | **Mức độ hoàn thành** | **Đánh giá của nhóm** |
| 18120518 – Phượng | * Giao diện cho phép thêm quyền/ Lấy lại quyền của user/ role. * MAC 1 chính sách và giao diện * Mã hóa + giao diện * Đưa ra các chính sách bảo mật | 100% | 10/10 |
| 18120538 - Sơn | * Giao diện xem danh sách tên các đối tượng bạn đã tạo trong trong CSDL (user, role, table, view,...) * Giao diện cho phép Admin thêm mới đối tượng (table, role, user, …) * RBAC + DAC chính sách và giao diện * VPD chính sách và giao diện | 100% | 10/10 |
| 18120580 – Thọ | * Giao diện cho phép xem quyền của một chủ thể. * Audit cơ bản và FGA (2 chính sách) và giao diện * Lược đồ CSDL, liệt kê chính sách bảo mật, phân tích và phân loại * Đưa ra các chính sách bảo mật | 100% | 10/10 |

# MÔ TẢ ĐỒ ÁN CUỐI KỲ

**Phân hệ 1:** Hệ thống dành cho người quản trị bảo mật

* Yêu cầu: Xây dựng giao diện cho phép người quản trị
* Xem danh sách các đối tượng hiện có trên CSDL (user, role, table, view, ....)
* Thêm mới đối tượng (table, user, role, ...)
* Phân quyền/ lấy lại quyền của một user/ role.
* Xem quyền của một chủ thể cụ thể.

**Phân hệ 2:** Giao diện ứng dụng quản lý thông tin của một bệnh viện.

* Ta sẽ liệt kê, phân tích các chính sách bảo mật phù hợp với hệ thống, và cài đặt chúng theo các cơ chế bảo mật đã học (Điều khiển truy cập - Access Control (DAC, RBAC, MAC), VPD, Mã hóa - Encryption, Auditing).

# KẾT QUẢ

## Phân hệ 1 – Hệ thống dành cho người quản trị cơ sở dữ liệu

### **Bảng danh sách các yêu cầu đã thực hiện:**

|  |  |  |
| --- | --- | --- |
| **STT** | **Yêu cầu** |  |
| 1 | Xem danh sách các đối tượng hiện có trên cơ sở dữ liệu (user, role, table, view,…). | ✓ |
| 2 | Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu. | ✓ |
| 3 | Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role. | ✓ |
| 4 | Cho phép thực hiện việc cấp quyền: cấp quyền cho user, cấp quyền cho role, cấp role cho user. | ✓ |
| 5 | Quá trình cấp quyền có tùy chọn là có cho phép người được cấp quyền có thể cấp quyền đó cho user/ role khác hay không (có chỉ định WITH GRANT OPTION hay không). | ✓ |
| 6 | Quyền, select, update thì cho phép phân quyền tinh đến mức cột; quyền insert, delete thì không. | ✓ |
| 7 | Cho phép thu hồi quyền từ user/ role. | ✓ |
| 8 | Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền. | ✓ |
| 9 | Cho phép chỉnh sửa quyền của user/ role. | ✓ |
| 10 | Admin có quyền enable/ disable việc ghi nhật ký toàn hệ thống. | ✓ |
| 11 | Admin được chỉ định ghi nhật ký của những hành động thực hiện bởi những user nào trên những đối tượng cụ thể.   * Các hành động đó là: đăng nhập, thay đổi thông tin user account, select, insert, update, delete, execute. * Các đối tượng là table, view, stored procedure, function. | ✓ |
| 12 | Admin được quyền chọn ghi nhật ký hành động được thực hiện thành công hay không thành công. | ✓ |
| 13 | Kiểm tra dữ liệu nhật ký hệ thống. | ✓ |
| 14 | Đề ra một số kịch bản theo dõi hệ thống để phân tích dữ liệu nhật ký. | ✓ |
| 15 | Giao diện cho người quản trị. | ✓ |

### **Giao diện dành cho người quản trị hệ cơ sở dữ liệu**

1. **Giao diện xem danh sách tên các đối tượng bạn đã tạo trong CSDL (user, role, table, view,...)**

Table

Description automatically generated

*Hình 1. Giao diện xem danh sách tên các User*

Graphical user interface

Description automatically generated

*Hình 2. Giao diện xem danh sách tên các Role*

Graphical user interface, table

Description automatically generated

*Hình 3. Giao diện xem danh sách tên các Table*

Table

Description automatically generated

*Hình 4. Giao diện xem danh sách tên các View*

1. **Giao diện cho phép Admin thêm mới đối tượng (table, role, user, …)**

*Graphical user interface, application

Description automatically generated*

*Hình 5. Giao diện cho phép Admin thêm User*

*Graphical user interface, text, application, email

Description automatically generated*

*Hình 6. Giao diện cho phép Admin thêm Role*

*Graphical user interface, application

Description automatically generated*

*Hình 7. Giao diện cho phép Admin thêm Table*

1. **Giao diện cho phép thêm quyền/ Lấy lại quyền của user/ role.**

Graphical user interface

Description automatically generated

*Hình 8. Giao diện cho phép thêm quyền của User*

Graphical user interface, application, table

Description automatically generated

*Hình 9. Giao diện cho phép thêm quyền của Role*

Graphical user interface, application

Description automatically generated

*Hình 10. Giao diện cho phép lấy lại quyền của User*

Graphical user interface, table

Description automatically generated

*Hình 11. Giao diện cho phép lấy lại quyền của Role*

1. **Xem quyền của một chủ thể cụ thể.**

**Graphical user interface, application

Description automatically generated**

*Hình 12. Giao diện xem quyền của một User*

**Graphical user interface, application

Description automatically generated**

*Hình 13. Giao diện xem quyền của một Role*

## Phân hệ 2 – Quản lý thông tin của một bệnh viện

### **Lược đồ cơ sở dữ liệu**

**BENHNHAN** (MaBenhNhan, HoTen, NgaySinh, DiaChi, SoDienThoai, CMND, BHYT)

**HOSOBENHAN**(MaKhamBenh,NgayKhamBenh,TinhTrangBanDau,KetLuanCuaBacSi, BenhNhan, NhanVienDieuPhoi,BacSiDieuTri)

**THUOC(**MaThuoc,TenThuoc,DonGia,LuuY,DonViTinh)

**DONTHUOC**(MaDonThuoc,MaKhamBenh)

**CT\_DONTHUOC(**MaDonThuoc,MaThuoc,SoLuong,LieuDung,MoTa)

**NHANVIEN**(MaNhanVien,HoTen,DiaChi,NgaySinh,CMND,Luong,GioiTinh, PhuCap, DonVi)

**CHAMCONG**(MaNhanVien,Thang,Nam,SoNgayCong**)**

**PHIEULUONG**(MaNhanVien,Thang,Nam,TongLuong,NgayLap,NVLP)

**HOADONDICHVU**(MaHDDV,NgayLapHoaDon,TongTien,MaKhamBenh, NVPT)

**HOADONTIENTHUOC**(MaHDTT,MaDonThuoc,NgayLapHoaDon,TongTien,NVPT)

**CT\_HOADONDICHVU**(MaHDDV,MaDichVu)

**DICHVU**(MaDichVu,TenDichVu,DonGia)

**DONVI**(MaDonVi,TenDonVi)

**HOSODICHVU**(MaKhamBenh,MaDichVu,NgayGio,KetLuan,KyThuatVien)

### **Các chính sách bảo mật**

|  |  |  |
| --- | --- | --- |
| **TABLE** | **Chính sách** | **Phân loại** |
| **NHANVIEN** | Nhân viên Quản lý tài nguyên nhân sự được thêm, xóa, sửa bảng NHANVIEN | DAC / RBAC |
| Nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ và nhân viên Kế toán được xem hết bảng NHANVIEN | DAC / RBAC |
| Mỗi nhân viên chỉ được xem thông tin riêng của họ ngoại trừ những trường hợp trên, và chỉ được chỉnh sửa họ tên, địa chỉ, ngày sinh, giới tính, cmnd của họ | VPD |
| **HOSOBENHAN** | Nhân viên Quản lý tài nguyên nhân sự, Quản lý tài vụ, Quản lý chuyên môn, Bác sĩ và Tiếp tân được phép xem trên bảng Hồ sơ bệnh án | DAC / RBAC |
| Tiếp tân được xóa, sửa trên bảng Hồ sơ bệnh án mà do chính nhân viên đó tiếp nhận, lưu ý trừ cột Kết luận của bác sĩ | VPD |
| Bác sĩ được quyền xem trên bảng Hồ sơ bệnh án, những hồ sơ bệnh án mà do chính bác sĩ điều trị, và được phép cập nhật cột Kết luận của bác sĩ của những hồ sơ bệnh án mà do chính bác sĩ điều trị. | VPD |
| **CHAMCONG** | Nhân viên chỉ được xem thông tin chấm công của chính nhân viên đó. | VPD |
| Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, và nhân viên Kế toán được xem toàn bảng Chấm công | DAC / RBAC |
| Nhân viên Quản lý tài nguyên nhân sự được thêm, xóa, sửa trên bảng Chấm công | DAC / RBAC |
| **DONVI** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng Đơn vị | DAC / RBAC |
| Nhân viên Quản lý tài nguyên nhân sự được thêm, xóa, sửa trên bảng Đơn vị | DAC / RBAC |
| **BENHNHAN** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, nhân viên Tiếp tân, nhân viên Tài vụ, nhân viên Bán thuốc được xem bảng Bệnh nhân | DAC / RBAC |
| Nhân viên Tiếp tân được thêm, xóa, sửa trên bảng Bệnh nhân | DAC / RBAC |
| **HOSODICHVU** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, nhân viên Tài vụ, nhân viên Tiếp tân, Kỹ thuật viên, Bác sĩ được xem bảng Hồ sơ dịch vụ | DAC / RBAC |
| Nhân viên Tiếp tân được xem **Hồ sơ dịch vụ** của Hồ sơ bệnh án mà chính nhân viên đó điều phối  Nhân viên Tiếp tân được sửa trên cột ***Kỹ Thuật viên*** trong bảng **Hồ sơ dịch vụ** mà chính nhân viên đó điều phối | VPD |
| Bác sĩ được xem, thêm, sửa *Mã khám bệnh, mã dịch vụ và ngày giờ* trên bảng **Hồ sơ dịch vụ**mà do bác sĩ đó phụ trách  Bác sĩ được xóa **Hồ sơ dịch vụ** mà do bác sĩ đó phụ trách | VPD |
| Kỹ thuật viên được xem, sửa cột ***Kết luận*** của **Hồ sơ dịch vụ** mà chính nhân viên đó tiếp nhận | VPD |
| **DONTHUOC** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, nhân viên Bán thuốc được xem bảng **Đơn thuốc** | DAC / RBAC |
| Bác sĩ được phép xem, thêm, xóa, sửa bảng **Đơn thuốc** của bệnh nhân mà chính bác sĩ đó điều trị | VPD |
| **CT\_DONTHUOC** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, nhân viên Bán thuốc được xem bảng **CT**\_**Đơn thuốc** | DAC / RBAC |
| Bác sĩ được phép xem, thêm, xóa, sửa bảng **CT**\_**Đơn thuốc** của bệnh nhân mà chính bác sĩ đó điều trị | VPD |
| **HOADONDICHVU** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng **Hóa đơn dịch vụ** | DAC / RBAC |
| Nhân viên Tài vụ được thêm bảng **Hóa đơn dịch vụ**  Nhân viên Tài vụ được xem, sửa, xóa trên bảng **Hóa đơn dịch vụ** do chính nhân viên đó tạo ra | VPD |
| **CT\_HOADONDICHVU** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng **CT\_Hóa đơn dịch vụ** | DAC / RBAC |
| Nhân viên tài vụ được thêm trên bảng **CT\_Hóa đơn dịch vụ** của Hóa đơn dịch vụ mà chính nhân viên đó lặp  Nhân viên tài vụ được xem, xóa, sửa **CT\_Hóa đơn dịch vụ** mà chính nhân viên đó tạo ra | VPD |
| **HOADONTIENTHUOC** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng **Hóa đơn tiền thuốc** | DAC / RBAC |
| Nhân viên bán thuốc được thêm trong bảng **Hóa đơn tiền thuốc**  Nhân viên bán thuốc được xem, xóa, sửa **Hóa đơn tiền thuốc** mà chính nhân viên đó lặp | VPD |
| **PHIEULUONG** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng **Phiếu lương** | DAC / RBAC |
| Nhân viên Kế toán được thêm vào bảng **Phiếu lương**  Nhân viên Kế toán được xem, xóa, sửa **Phiếu lương** mà chính nhân viên đó lặp | VPD |
| Nhân viên chỉ được xem phiếu lương của chính họ, trừ những trường hợp trên | VPD |
| **DICHVU** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn được xem bảng **Dịch vụ**  Nhân viên Quản lý tài vụ được xem, thêm, xóa, sửa trên bảng **Dịch vụ** | DAC / RBAC |
| Bác sĩ được xem bảng **Dịch vụ** trừ thuộc tính Đơn giá  Kỹ thuật viên được xem bảng **Dịch vụ** trừ thuộc tính Đơn giá | VPD |
| **THUOC** | Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Bán thuốc được xem bảng **Thuốc**  Nhân viên Quản lý Tài vụ được xem, thêm, xóa, sửa trên bảng **Thuốc** | DAC / RBAC |
| Bác sĩ được xem bảng Thuốc trừ thuộc tính Đơn Giá | VPD |

#### Cơ chế DAC, RBAC, VPD

1. **BẢNG NHANVIEN**
2. Nhân viên Quản lý tài nguyên nhân sự được thêm, xóa, sửa bảng NHANVIEN

* DAC / RBAC

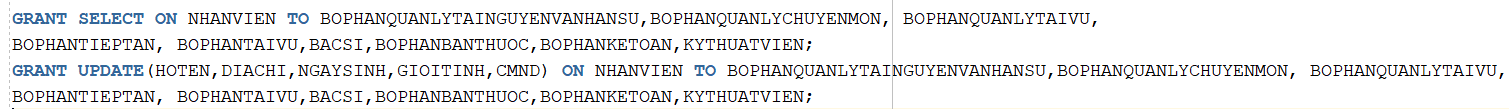


1. Nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ và nhân viên Kế toán được xem hết bảng NHANVIEN

* DAC / RBAC

1. Mỗi nhân viên chỉ được xem thông tin riêng của họ ngoại trừ những trường hợp trên, và chỉ được chỉnh sửa họ tên, địa chỉ, ngày sinh, giới tính, cmnd của họ

* VPD

*Hình A1. Ta gán quyền Select trên bảng Nhân viên cho toàn bộ nhân viên và quyền Update các cột như đã miêu tả ở phần c*

*Graphical user interface, text, application, email

Description automatically generated*

*Hình A2. VPD được áp dụng cho việc mỗi nhân viên chỉ được xem thông tin cá nhân của mình*

* Tạo hàm chính sách **“Xem thông tin nhân viên”** có vị từ trả về là **đúng “1=1”** đối với những User có quyền xem toàn bộ bảng Nhân viên (*người quản trị CSDL - ADMINBV, nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý tài vụ, nhân viên Quản lý chuyên môn, nhân viên Kế toán*). Còn đối với những User khác chỉ được xem thông tin của chính mình thì trả về vị từ **Mã nhân viên = User đang đăng nhập.**
* Gán hàm chính sách lên bảng dữ liệu cần bảo vệ, với schema của ADMINBV áp dụng với câu lệnh ***Select*** trên bảng **Nhân viên**

Graphical user interface, text, application, email

Description automatically generated

*Hình A3. VPD tiếp tục được áp dụng cho việc mỗi nhân viên được chỉnh sửa thông tin cá nhân của chính mình*

* Tạo hàm chính sách **Sửa thông tin nhân viên** có vị từ trả về **đúng “1=1”** đối với những User có quyền sửa toàn bộ bảng Nhân viên (*người quản trị CSDL – ADMINBV, nhân viên Quản lý tài nguyên nhân sự).* Còn đối với những User khác chỉ được sửa thông tin của chính mình thì trả về vị từ **Mã nhân viên = User đang đăng nhập.**
* Gán hàm chính sách lên bảng dữ liệu cần bảo vệ, với schema của ADMINBV áp dụng với câu lệnh ***Update*** trên bảng **Nhân viên**

*Graphical user interface

Description automatically generated*

*Hình A4. Giao diện chỉnh sửa thông tin cá nhân của nhân viên*

Graphical user interface

Description automatically generated

*Hình A5. Giao diện xem thông tin nhân sự*

Graphical user interface

Description automatically generated

*Hình A6. Giao diện chỉnh sửa thông tin cá nhân của toàn bộ nhân viên của Nhân viên Quản lý tài nguyên nhân sự*

1. **BẢNG HOSOBENHAN**
2. Nhân viên Quản lý tài nguyên nhân sự, Quản lý tài vụ, Quản lý chuyên môn, Bác sĩ và Tiếp tân được phép xem trên **bảng Hồ sơ bệnh án**

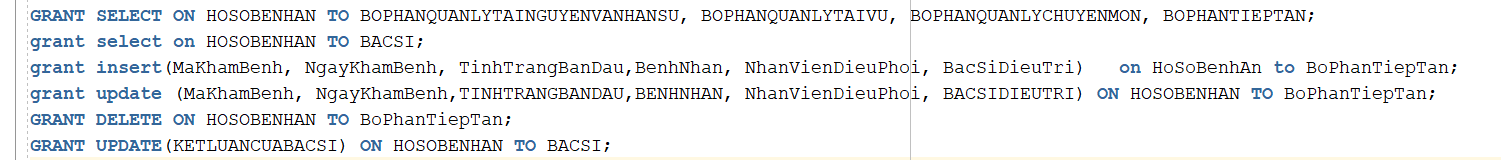
* **DAC / RBAC**

1. Tiếp tân được xem, xóa, sửa trên bảng **Hồ sơ bệnh án** mà do chính nhân viên đó tiếp nhận, lưu ý trừ cột ***Kết luận của bác sĩ***

* **VPD**

1. Bác sĩ được quyền *xem* trên bảng Hồ sơ bệnh án, những hồ sơ bệnh án mà do chính bác sĩ điều trị, và được phép *cập nhật* cột ***Kết luận của bác sĩ*** của những hồ sơ bệnh án mà do chính bác sĩ điều trị.

* **VPD**

****

*Hình B1. Những câu lệnh cấp quyền phù hợp với yêu cầu của 3 ý trên*

Text

Description automatically generated

*Hình B2. Tạo hàm chính sách xem hồ sơ bệnh án*

*Text

Description automatically generated*

*Hình B3. Gán hàm chính sách lên bảng dữ liệu cần bảo vệ*

* Tạo hàm chính sách **Xem HSBA** có vị từ trả về là **đúng “1=1”** đối với những User có quyền xem toàn bộ trên bảng HSBA (*người quản trị CSDL – ADMINBV, nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý tài vụ, nhân viên Quản lý chuyên môn, nhân viên tiếp tân)*. Còn đối với Bác sĩ chỉ được xem những HSBA mà mình điều trị thì trả về vị từ Bác sĩ điều trị = User đang đăng nhập
* Gán hàm chính sách lên bảng dữ liệu cần bảo vệ, với schema của ADMINBV áp dụng với câu lệnh ***Select*** trên bảng **Hồ sơ bệnh án**

**Text, timeline

Description automatically generated**

*Hình B4. Tạo hàm chính sách sửa hồ sơ bệnh án*

*Text

Description automatically generated*

*Hình B5. Gán hàm chính sách lên bảng dữ liệu cần bảo vệ*

* Tạo hàm chính sách **Sửa HSBA** có vị từ trả về là **đúng “1=1”** đối với User có quyền sửa HSBA (*người quản trị CSDL – ADMINBV***).** Còn đối với nhân viên Tiếp tân thì chỉ chỉnh sửa những HSBA mà nhân viên đó tiếp nhận thì trả về vị từ là Nhân viên điều phối = User đang đăng nhập. Đối với bác sĩ thì có quyền chỉnh sửa những HSBA mà bác sĩ đó điều trị thì trả về vị từ là Bác sĩ điều trị = User đang đăng nhập
* Gán hàm chính sách lên bảng dữ liệu cần bảo vệ, với schema của ADMINBV áp dụng với câu lệnh ***insert, update, delete*** trên bảng **Hồ sơ bệnh án**

Table

Description automatically generated

*Hình B6. Giao diện xem hồ sơ bệnh án*

*Graphical user interface, application

Description automatically generated*

*Hình B7. Giao diện thêm, xóa, sửa hồ sơ bệnh án*

Graphical user interface, application

Description automatically generated

*Hình B8. Giao diện cập nhật Kết luận của Bác Sĩ*

1. **BẢNG CHẤM CÔNG**
2. Nhân viên chỉ được xem thông tin chấm công của chính nhân viên đó.

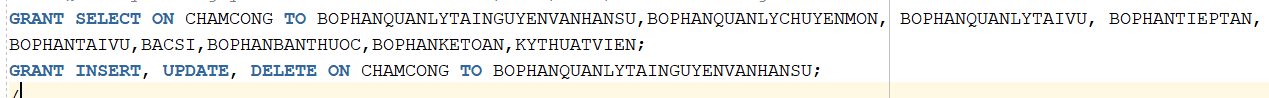
* **VPD**

1. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, và nhân viên Kế toán được xem toàn bảng **Chấm công**

* **DAC / RBAC**

1. Nhân viên Quản lý tài nguyên nhân sự được thêm, xóa, sửa trên bảng **Chấm công**

* **DAC / RBAC**

****

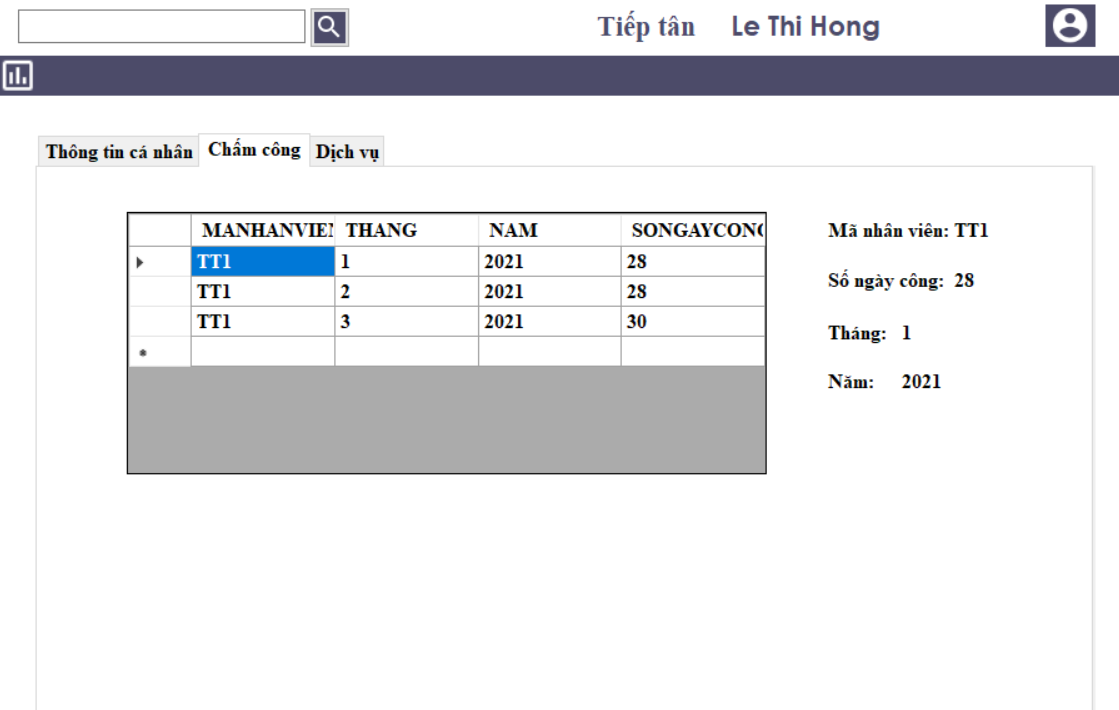
*Hình C1. Những câu lệnh cấp quyền phù hợp với yêu cầu của 3 ý trên*

*Graphical user interface, text, application

Description automatically generated*

*Hình C2. VPD được áp dụng cho việc mỗi nhân viên chỉ được xem thông tin chấm công của mình*

* Tạo hàm chính sách **Xem thông tin chấm công** có vị từ trả về là **đúng “1=1”** đối với những User có quyền xem toàn bộ bảng Chấm công (*người quản trị CSDL - ADMINBV, nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý tài vụ, nhân viên Quản lý chuyên môn, nhân viên Kế toán*). Còn đối với các User còn lại chỉ được xem thông tin Chấm công của chính họ thì trả về vị từ là Mã nhân viên = User đang đăng nhập.
* Gán hàm chính sách lên bảng dữ liệu cần bảo vệ, với schema của ADMINBV áp dụng với câu lệnh ***Select*** trên bảng **Chấm công**.



*Hình C3. Giao diện chấm công của riêng mỗi cá nhân*

Table

Description automatically generated

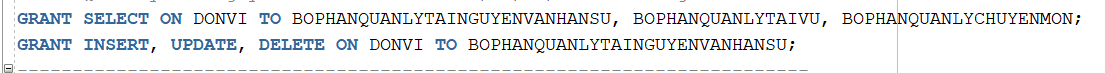
*Hình C4. Giao diện thêm, xóa, sửa bảng Chấm công*

1. **BẢNG ĐƠN VỊ**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng Đơn vị

* **DAC / RBAC**

1. Nhân viên Quản lý tài nguyên nhân sự được thêm, xóa, sửa trên bảng Đơn vị

* **DAC / RBAC**

****

**Graphical user interface, application

Description automatically generated**

*Hình D1. Giao diện bảng Đơn vị*

Graphical user interface, application

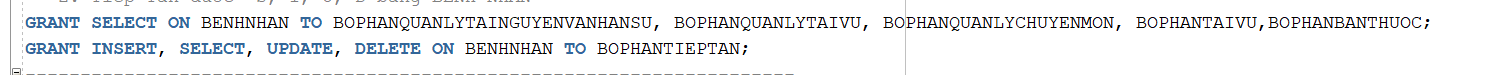
Description automatically generated

*Hình D2. Giao diện thêm, xóa, sửa bảng Đơn vị*

1. **BẢNG BỆNH NHÂN**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, nhân viên Tiếp tân, nhân viên Tài vụ, nhân viên Bán thuốc được xem bảng **Bệnh nhân**

* **DAC / RBAC**

1. Nhân viên Tiếp tân được thêm, xóa, sửa trên bảng **Bệnh nhân**

* **DAC / RBAC**
* ****

**Table

Description automatically generated**

*Hình E1. Giao diện bảng Bệnh nhân*

*Graphical user interface

Description automatically generated with medium confidence*

*Hình E2. Giao diện thêm, xóa, sửa bảng Bệnh nhân*

1. **BẢNG DỊCH VỤ**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn được xem bảng Dịch vụ

Nhân viên Quản lý tài vụ được xem, thêm, xóa, sửa trên bảng **Dịch vụ**

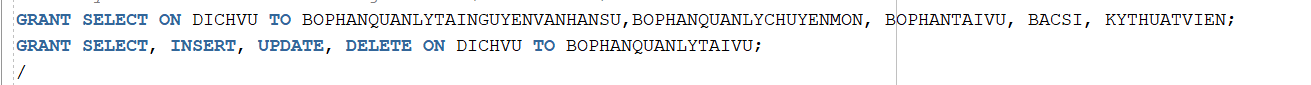
* **DAC / RBAC**

1. Bác sĩ được xem bảng Dịch vụ trừ thuộc tính Đơn giá

* **VPD**

1. Kỹ thuật viên được xem bảng Dịch vụ trừ thuộc tính Đơn giá

* **VPD**

****

*Hình F1. Những câu lệnh cấp quyền phù hợp với yêu cầu của 3 ý trên*

*Graphical user interface, text, application, email

Description automatically generated*

*Hình F2. VPD được áp dụng cho việc Bác sĩ, Kỹ thuật viên được xem bảng Dịch vụ (trừ thuộc tính Đơn giá)*

* Tạo hàm chính sách **Xem dịch vụ** có vị từ trả về là **đúng “1=1”** đối với những User có quyền xem toàn bộ bảng Dịch vụ - được xem cột Đơn giá - (*người quản trị CSDL - ADMINBV, nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý tài vụ, nhân viên Quản lý chuyên môn, nhân viên Tài vụ*) . Còn đối với Bác sĩ và Kỹ thuật viên – không xem được cột Đơn giá – thì vị từ trả về là **sai “1=0”**
* Gán hàm chính sách lên bảng dữ liệu cần bảo vệ, với schema của ADMINBV áp dụng với câu lệnh ***Select*** trên bảng **Dịch vụ.**

**Table

Description automatically generated**

*Hình F3. Giao diện dịch vụ dành cho Bác Sĩ và Kỹ thuật viên*

*Graphical user interface, table

Description automatically generated*

*Hình F3. Giao diện dịch vụ dành cho nhân viên Quản lý tài vụ*

1. **BẢNG HỒ SƠ DỊCH VỤ**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, nhân viên Tài vụ, nhân viên Tiếp tân, Kỹ thuật viên, Bác sĩ được xem bảng **Hồ sơ dịch vụ**

* **DAC / RBAC**

1. Nhân viên Tiếp tân được xem **Hồ sơ dịch vụ** của Hồ sơ bệnh án mà chính nhân viên đó điều phối

Nhân viên Tiếp tân được sửa trên cột Kỹ Thuật viên trong bảng **Hồ sơ dịch vụ** mà chính nhân viên đó điều phối

* **VPD**

1. Bác sĩ được xem, thêm, sửa Mã khám bệnh, mã dịch vụ và ngày giờ trên bảng **Hồ sơ dịch vụ** mà do bác sĩ đó phụ trách

Bác sĩ được xóa **Hồ sơ dịch vụ** mà do bác sĩ đó phụ trách

* **VPD**

1. Kỹ thuật viên được xem, sửa cột ***Kết luận*** của **Hồ sơ dịch vụ** mà chính nhân viên đó tiếp nhận

* **VPD**

1. **BẢNG ĐƠN THUỐC**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, nhân viên Bán thuốc được xem bảng **Đơn thuốc**

* **DAC / RBAC**

1. Bác sĩ được phép xem, thêm, xóa, sửa bảng **Đơn thuốc** của bệnh nhân mà chính bác sĩ đó điều trị

* **VPD**

1. **BẢNG CT ĐƠN THUỐC**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ, nhân viên Bán thuốc được xem bảng **CT**\_**Đơn thuốc**

* **DAC / RBAC**

1. Bác sĩ được phép xem, thêm, xóa, sửa bảng **CT**\_**Đơn thuốc** của bệnh nhân mà chính bác sĩ đó điều trị

* **VPD**

1. **BẢNG HÓA ĐƠN DỊCH VỤ**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng **Hóa đơn dịch vụ**

* **DAC / RBAC**

1. Nhân viên Tài vụ được thêm bảng **Hóa đơn dịch vụ**

Nhân viên Tài vụ được xem, sửa, xóa trên bảng **Hóa đơn dịch vụ** do chính nhân viên đó tạo ra

* **VPD**

1. **BẢNG CT HÓA ĐƠN DỊCH VỤ**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng **CT\_Hóa đơn dịch vụ**

* **DAC / RBAC**

1. Nhân viên tài vụ được thêm trên bảng **CT\_Hóa đơn dịch vụ** của Hóa đơn dịch vụ mà chính nhân viên đó lặp

Nhân viên tài vụ được xem, xóa, sửa **CT\_Hóa đơn dịch vụ** mà chính nhân viên đó tạo ra

* **VPD**

1. **BẢNG HÓA ĐƠN TIỀN THUỐC**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng **Hóa đơn tiền thuốc**

* **DAC / RBAC**

1. Nhân viên bán thuốc được thêm trong bảng **Hóa đơn tiền thuốc**

Nhân viên bán thuốc được xem, xóa, sửa **Hóa đơn tiền thuốc** mà chính nhân viên đó lặp

* **VPD**

1. **BẢNG PHIẾU LƯƠNG**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Quản lý Tài vụ được xem bảng **Phiếu lương**

* **DAC / RBAC**

1. Nhân viên Kế toán được thêm vào bảng **Phiếu lương**

Nhân viên Kế toán được xem, xóa, sửa **Phiếu lương** mà chính nhân viên đó lặp

* **VPD**

1. Nhân viên chỉ được xem phiếu lương của chính họ, trừ những trường hợp trên

* **VPD**

1. **BẢNG THUỐC**
2. Nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý chuyên môn, nhân viên Bán thuốc được xem bảng **Thuốc**

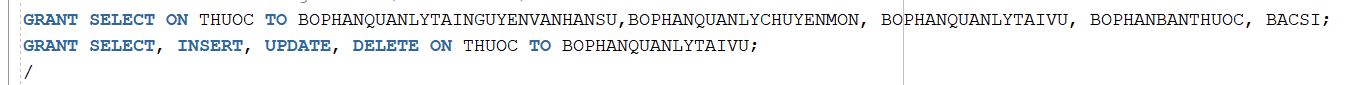
* **DAC / RBAC**

1. Nhân viên Quản lý Tài vụ được xem, thêm, xóa, sửa trên bảng **Thuốc**

* **DAC / RBAC**

1. Bác sĩ được xem bảng **Thuốc** trừ thuộc tính Đơn Giá VPD

* **VPD**

****

*Hình N1. Những câu lệnh cấp quyền phù hợp với yêu cầu của 3 ý trên*

*Graphical user interface, text, application

Description automatically generated*

*Hình N2. VPD được áp dụng cho việc Bác sĩ được xem bảng Thuốc(trừ thuộc tính Đơn giá)*

* Tạo hàm chính sách **Xem thuốc** có vị từ trả về là **đúng “1=1”** đối với những User có quyền xem toàn bộ bảng Thuốc - được xem cột Đơn giá - (*người quản trị CSDL - ADMINBV, nhân viên Quản lý tài nguyên nhân sự, nhân viên Quản lý tài vụ, nhân viên Quản lý chuyên môn, nhân viên Tài vụ*) . Còn đối với Bác sĩ và Kỹ thuật viên – không xem được cột Đơn giá – thì vị từ trả về là **sai “1=0”**
* Gán hàm chính sách lên bảng dữ liệu cần bảo vệ, với schema của ADMINBV áp dụng với câu lệnh ***Select*** trên bảng **Thuốc.**

#### Cơ chế MAC (OLS)

* Mỗi nhân viên có cấp bậc, phòng ban, cơ sở khác nhau thì sẽ xem được những thông báo khác nhau.

=> Sử dụng MAC. Vì những cơ chế bảo mật khác (RBAC, VPD,…) phải căn cứ vào nội dung của dữ liệu, còn MAC căn cứ vào mục đích của dữ liệu, tức là thông báo muốn phát tán đến ai để gán nhãn cho phù hợp.

* Các bước thực hiện:

**Bước 1: Tạo bảng Thông báo và phân quyền cho các nhân viên xem thông báo**

**+** Đăng nhập vào DBA (ADMINBV) và tạo bảng ThongBao

**+** Grant select on ThongBao to QLTNNS1,QLTV1,QLCM1,…

**Bước 2: Tạo chính sách và cấp quyền thực thi chính sách**

**+** Đăng nhập tài khoản LBACSYS

**+** Tạo chính sách tên XemThongBao

* Cấp một số quyền cho DBA (ADMINBV) để có thể thực thi chính sách

**Bước 3: Tạo Level, Compartment, Group, Label và gán nhãn cho các User**

|  |  |  |
| --- | --- | --- |
| **CÁC CẤP** | **LEVEL** | **LEVEL NUM** |
| Điều hành | DH | 9000 |
| Quản lý | QL | 8000 |
| Nhân viên | NV | 7000 |

|  |  |  |
| --- | --- | --- |
| **PHÒNG BAN** | **COMPARTMENT** | **COMP NUM** |
| Tài nguyên nhân sự | NS | 5000 |
| Tài vụ | TV | 1000 |
| Kế toán | KT | 100 |
| Chuyên môn | CM | 10 |

|  |  |  |
| --- | --- | --- |
| **CƠ SỞ** | **GROUP** | **GROUP NUM** |
| Hồ Chí Minh | HCM | 110 |
| Hà Nội | HN | 220 |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **THÔNG BÁO** | **LABEL** | **LABEL TAG** |
| 1 | Thông báo lịch nghỉ tết Nguyên đán năm 2020 | NV | 10000 |
| 2 | Nhân viên phòng Kế toán tiến hành tính lương tháng 8 | NV:KT | 11000 |
| 3 | Nhân viên phòng Tài nguyên nhân sự chuẩn bị đợt tuyển dụng | NV:NS | 11100 |
| 4 | Nhân viên phòng Tài vụ gửi báo cáo thống kê chi phí dịch vụ | NV:TV | 11200 |
| 5 | Danh sách nhân viên được tăng lương phòng Kế toán cơ sở Hà Nội | NV:KT:HN | 11010 |
| 6 | Nhân viên Tài vụ cơ sở Hà Nội họp thường niên | NV:TV:HN | 11110 |
| 7 | Các quản lý gửi báo cáo về nhu cầu tuyển thêm nhân sự của phòng mình | QL | 20000 |
| 8 | Quản lý Kế toán gửi báo cáo lương tháng 8 | QL:KT | 21000 |
| 9 | Quản lý Tài nguyên nhân sự gửi báo cáo nhân sự năm 2021 | QL:NS | 21100 |
| 10 | Quản lý phòng Tài vụ cơ sở Hà Nội họp gấp | QL:TV:HN | 21210 |
| 11 | Thông báo họp ban Điều hành | DH | 30000 |

|  |  |  |
| --- | --- | --- |
| **USER NAME** | **USER LABEL** | **LABEL TAG** |
| QLCM1 | DH:CM,KT,TV,NS:HCM,HN | 32000 |
| QLTV1 | QL:TV:HN | 21210 |
| KT1 | QL:KT:HCM | 21020 |
| QLTNNS1 | QL:NS:HN | 21110 |
| KT2 | NV:KT:HCM | 11020 |
| TV1 | NV:TV:HCM | 11220 |
| TV2 | NV:TV:HN | 11110 |

Ví dụ:

**- Tạo Level**

*sa\_components.create\_level*

*(policy\_name => 'xemthongbao',*

*long\_name => 'Dieu hanh',*

*short\_name => 'DH',*

*level\_num => 9000);*

**- Tạo Compartment**

sa\_components.create\_compartment

(policy\_name => 'xemthongbao',

long\_name => 'Tai nguyen nhan su',

short\_name => 'NS',

comp\_num => 5000);

**- Tạo Group**

*sa\_components.CREATE\_GROUP*

*(policy\_name => 'xemthongbao',*

*long\_name => 'Ho Chi Minh',*

*short\_name => 'HCM',*

*group\_num => 110,*

*parent\_name => null);*

**- Tạo Label**

*sa\_label\_admin.create\_label*

*(policy\_name => 'xemthongbao',*

*label\_tag =>10000 ,*

*label\_value => 'NV'); -- TB1*

**- Gán nhãn cho User**

*sa\_user\_admin.set\_user\_labels*

*(policy\_name => 'xemthongbao',*

*user\_name => 'ADMINBV', -- Dieu hanh*

*max\_read\_label => 'DH:CM,KT,TV,NS:HCM,HN');*

**Bước 4: Áp dụng chính sách cho bảng Thông báo**

* Ban đầu, áp dụng cơ chế NO\_CONTROL để có thể insert dữ liệu vào bảng thông báo

**Bước 5: Insert dữ liệu cho bảng Thông báo cùng nhãn phù hợp**

* Ví dụ:

*INSERT INTO ADMINBV.THONGBAO VALUES('Thong bao hop ban Dieu hanh',char\_to\_label('xemthongbao', 'DH'));*

*INSERT INTO ADMINBV.THONGBAO VALUES('Danh sach nhan vien duoc tang luong phong Ke toan co so Ha Noi',char\_to\_label('xemthongbao', 'NV:KT:HN'));*

**Bước 6: Áp dụng chính sách với cơ chế phù hợp**

* Sau khi insert dữ liệu vào bảng thông báo, ta áp dụng cơ chế LABEL\_DEFAULT,READ\_CONTROL để người dùng có nhãn nào thì sẽ đọc được thông báo có nhãn phù hợp

**Bước 7: Test**

* QLCM1 **: DH:KT,TV,NS:HCM,HN**

|  |  |  |
| --- | --- | --- |
|  | **THÔNG BÁO** | **LABEL** |
| 1 | Thông báo lịch nghỉ tết Nguyên đán năm 2020 | NV |
| 2 | Nhân viên phòng Kế toán tiến hành tính lương tháng 8 | NV:KT |
| 3 | Nhân viên phòng Tài nguyên nhân sự chuẩn bị đợt tuyển dụng | NV:NS |
| 4 | Nhân viên phòng Tài vụ gửi báo cáo thống kê chi phí dịch vụ | NV:TV |
| 5 | Danh sách nhân viên được tăng lương phòng Kế toán cơ sở Hà Nội | NV:KT:HN |
| 6 | Nhân viên Tài vụ cơ sở Hà Nội họp thường niên | NV:TV:HN |
| 7 | Các quản lý gửi báo cáo về nhu cầu tuyển thêm nhân sự của phòng mình | QL |
| 8 | Quản lý Kế toán gửi báo cáo lương tháng 8 | QL:KT |
| 9 | Quản lý Tài nguyên nhân sự gửi báo cáo nhân sự năm 2021 | QL:NS |
| 10 | Quản lý phòng Tài vụ cơ sở Hà Nội họp gấp | QL:TV:HN |
| 11 | Thông báo họp ban Điều hành | DH |

* QLTV1 **:  QL:TV:HN**

|  |  |  |
| --- | --- | --- |
|  | THÔNG BÁO | LABEL |
| 1 | Thông báo lịch nghỉ tết Nguyên đán năm 2020 | NV |
| 2 | Nhân viên phòng Kế toán tiến hành tính lương tháng 8 | NV:KT |
| 3 | Nhân viên phòng Tài nguyên nhân sự chuẩn bị đợt tuyển dụng | NV:NS |
| 4 | Nhân viên phòng Tài vụ gửi báo cáo thống kê chi phí dịch vụ | NV:TV |
| 5 | Danh sách nhân viên được tăng lương phòng Kế toán cơ sở Hà Nội | NV:KT:HN |
| 6 | Nhân viên Tài vụ cơ sở Hà Nội họp thường niên | NV:TV:HN |
| 7 | Các quản lý gửi báo cáo về nhu cầu tuyển thêm nhân sự của phòng mình | QL |
| 8 | Quản lý Kế toán gửi báo cáo lương tháng 8 | QL:KT |
| 9 | Quản lý Tài nguyên nhân sự gửi báo cáo nhân sự năm 2021 | QL:NS |
| 10 | Quản lý phòng Tài vụ cơ sở Hà Nội họp gấp | QL:TV:HN |
| 11 | Thông báo họp ban Điều hành | DH |

* TK1: **QL:KT:HCM**

|  |  |  |
| --- | --- | --- |
|  | THÔNG BÁO | LABEL |
| 1 | Thông báo lịch nghỉ tết Nguyên đán năm 2020 | NV |
| 2 | Nhân viên phòng Kế toán tiến hành tính lương tháng 8 | NV:KT |
| 3 | Nhân viên phòng Tài nguyên nhân sự chuẩn bị đợt tuyển dụng | NV:NS |
| 4 | Nhân viên phòng Tài vụ gửi báo cáo thống kê chi phí dịch vụ | NV:TV |
| 5 | Danh sách nhân viên được tăng lương phòng Kế toán cơ sở Hà Nội | NV:KT:HN |
| 6 | Nhân viên Tài vụ cơ sở Hà Nội họp thường niên | NV:TV:HN |
| 7 | Các quản lý gửi báo cáo về nhu cầu tuyển thêm nhân sự của phòng mình | QL |
| 8 | Quản lý Kế toán gửi báo cáo lương tháng 8 | QL:KT |
| 9 | Quản lý Tài nguyên nhân sự gửi báo cáo nhân sự năm 2021 | QL:NS |
| 10 | Quản lý phòng Tài vụ cơ sở Hà Nội họp gấp | QL:TV:HN |
| 11 | Thông báo họp ban Điều hành | DH |

* KT2: **NV:KT:HCM**

|  |  |  |
| --- | --- | --- |
|  | THÔNG BÁO | LABEL |
| 1 | Thông báo lịch nghỉ tết Nguyên đán năm 2020 | NV |
| 2 | Nhân viên phòng Kế toán tiến hành tính lương tháng 8 | NV:KT |
| 3 | Nhân viên phòng Tài nguyên nhân sự chuẩn bị đợt tuyển dụng | NV:NS |
| 4 | Nhân viên phòng Tài vụ gửi báo cáo thống kê chi phí dịch vụ | NV:TV |
| 5 | Danh sách nhân viên được tăng lương phòng Kế toán cơ sở Hà Nội | NV:KT:HN |
| 6 | Nhân viên Tài vụ cơ sở Hà Nội họp thường niên | NV:TV:HN |
| 7 | Các quản lý gửi báo cáo về nhu cầu tuyển thêm nhân sự của phòng mình | QL |
| 8 | Quản lý Kế toán gửi báo cáo lương tháng 8 | QL:KT |
| 9 | Quản lý Tài nguyên nhân sự gửi báo cáo nhân sự năm 2021 | QL:NS |
| 10 | Quản lý phòng Tài vụ cơ sở Hà Nội họp gấp | QL:TV:HN |
| 11 | Thông báo họp ban Điều hành | DH |

#### Mã hóa

* CMND của bệnh nhân là trường thông tin nhạy cảm, cần được bảo vệ nên sẽ được mã hóa.
* Dùng thuật toán ENCRYPT\_AES256 với CHAIN\_CBC và PAD\_PKCS
* Key mã hóa dùng hàm RANDOMBYTES của package DBMS\_CRYPTO và được lưu trong bảng Khóa để quản lý

|  |  |
| --- | --- |
| Bước thực hiện | Script thực hiện |
| Tạo bảng Khoá chứa key mã hóa của mỗi dòng dữ liệu Bệnh Nhân | create table Khoa(  MaBN varchar2(10),  Key raw(32),  PPRIMARY KEY (MaBN) ); |
| Tạo package chứa các function encrypt, decrypt, | create or replace package package\_Crypt as  function f\_encrypt (p\_str in varchar2, p\_key in raw) return varchar2;  function f\_decrypt (p\_data in varchar2, p\_key in raw) return varchar2;  end;  /  create or replace package body package\_Crypt  as  --- ma hoa  function f\_encrypt (p\_str in varchar2, p\_key in raw)  return varchar2  as  encrypted\_str varchar2(200);  encrypted\_raw RAW (2000); -- stores encrypted binary text  encryption\_type PLS\_INTEGER := DBMS\_CRYPTO.ENCRYPT\_AES256+ DBMS\_CRYPTO.CHAIN\_CBC+ DBMS\_CRYPTO.PAD\_PKCS5;  begin  encrypted\_raw := DBMS\_CRYPTO.ENCRYPT  ( src => UTL\_I18N.STRING\_TO\_RAW (p\_str, 'AL32UTF8'),  typ => encryption\_type,  key => p\_key  );  encrypted\_str:= UTL\_RAW.CAST\_TO\_VARCHAR2(UTL\_ENCODE.base64\_encode(encrypted\_raw));  return encrypted\_str;  end;    --- giai ma  function f\_decrypt (p\_data in varchar2 , p\_key in raw)  return varchar2  as  decrypted\_raw RAW (2000); -- stores decrypted binary text  encryption\_type PLS\_INTEGER := DBMS\_CRYPTO.ENCRYPT\_AES256+ DBMS\_CRYPTO.CHAIN\_CBC+ DBMS\_CRYPTO.PAD\_PKCS5;  begin  decrypted\_raw := DBMS\_CRYPTO.DECRYPT(  src => UTL\_ENCODE.base64\_decode (UTL\_RAW.CAST\_TO\_RAW (p\_data)),  typ => encryption\_type,  key => p\_key  );  return UTL\_I18N.RAW\_TO\_CHAR (decrypted\_raw, 'AL32UTF8');  end;  end package\_Crypt; |
| Viết trigger sẽ mã hóa thông tin CMND khi có dữ liệu mới được insert. | create or replace trigger crypted\_BENHNHAN  before insert on ADMINBV.BENHNHAN\_ENC  for each row  declare key\_raw RAW(32);  begin  key\_raw := DBMS\_CRYPTO.RANDOMBYTES (32);  INSERT INTO KHOA VALUES (:new.MaBenhNhan , key\_raw);  :new.CMND := package\_Crypt.f\_encrypt(:new.CMND, key\_raw);  end; |
| Tạo view mã hóa hoặc đã giải mã và grant cho user phù hợp. | -- View chua du lieu ma hoa  create or replace view view\_BENHNHAN\_ENC as  select MABENHNHAN, HOTEN , ngaysinh , diachi , SODIENTHOAI ,cast(CMND as varchar(100)) CMND  from BENHNHAN\_ENC  -- View chua du lieu da giai ma  create or replace view VIEW\_BENHNHAN as  select MABENHNHAN, HOTEN , ngaysinh , diachi , SODIENTHOAI , cast( ADMINBV.package\_Crypt.f\_decrypt(CMND,KEY) as varchar2(200)) CMND  from BENHNHAN\_ENC, khoa  where MaBN= MaBenhNhan |

Graphical user interface, table

Description automatically generated

*Hình III\_1. Giao diện minh họa cho việc Mã hóa*

**- Để thay đổi khóa, ta phải giải mã dữ liệu bằng khóa cũ để lấy dữ liệu mã hóa bằng khóa mới**

|  |  |
| --- | --- |
| Bước thực hiện | Script thực hiện |
| Viết trigger sẽ mã hóa lại CMND khi cập nhật Key trong bảng Khoá | create or replace trigger UpdateKey  before update OF key on ADMINBV.KHOA  for each row  declare newcmnd varchar2(2000);  begin  select CMND into newcmnd from ADMINBV.BENHNHAN\_ENC where mabenhnhan=:new.mabn;  update BENHNHAN\_ENC set CMND= package\_Crypt.f\_encrypt(package\_Crypt.f\_decrypt(newcmnd, :old.key), :new.key) where MaBenhNhan= :new.MaBN;  end; |
| Tạo procedure để cập nhật Key trong bảng Khoá | create or replace procedure p\_updatekey(mbn in varchar2, newkey in raw)  as  begin  UPDATE KHOA SET KEY = newkey WHERE MABN=mbn;  end; |
| Tạo procedure để reset tất cả Key trong bảng Khoá | create or replace procedure p\_resetkey  as  cursor c\_khoa is select \* from khoa;  v\_khoa c\_khoa%rowtype;  begin  open c\_khoa;  loop  fetch c\_khoa into v\_khoa;  exit when c\_khoa%notfound;  update Khoa set key=DBMS\_CRYPTO.RANDOMBYTES (32) where mabn=v\_khoa.mabn;  end loop;  close c\_khoa;  end; |

#### Audit

1. **Quản lý standard audit trail**
   * 1. **Tham số khởi tạo ban đầu:**

* Cú pháp:

SHOW PARAMETER AUDIT;

Table

Description automatically generated with medium confidence

* + 1. **Kích hoạt standard audit:**
* Đăng nhập vào tài khoản sys với quyền sysdba
* Cú pháp:



* + 1. **Đối tượng sử dụng quyền audit:**
* Để sử dụng lệnh AUDIT thiết lập lựa chọn về câu lệnh và quyền thì bạn nhất thiết phải có quyền AUDIT SYSTEM. Còn để thiết lập các lựa chọn giám sát đối tượng bạn phải làm chủ đối tượng bị giám sát hay có quyền AUDIT ANY.

* + 1. **Audit trên một đối tương user cụ thể**
* Ví dụ

Aduit select on gdbv.benhnhan by QL1;

* + 1. **Lựa chọn audit hoạt động thực hiện thành công hay không thành công:**
* WHENEVER SUCCESSFUL/ WHENEVER NOT SUCCESSFUL
* WHENEVER SUCCESSFUL giám sát những lệnh thành công.
* WHENEVER NOT SUCCESSFUL giám sát những lệnh thất bại hay kết quả lỗi. Nếu loại bỏ hai mệnh đề này thì Oracle cũng sẽ ghi lại sự giám sát không quan tâm câu lệnh có thành công hay không.
  + 1. **Enable/disable audit:**
* Câu lệnh NOAUDIT để tắt các lựa chọn giám sát.
* Mệnh đề WHENEVER để tắt các giám sát đối với các câu lệnh được thực hiện thành công hay không thành công. Nếu không sử dụng mệnh đề đó thì chức năng giám sát sẽ tắt cả đối với trường hợp thành công hay thất bại.
  + 1. **Quản lý sự phát triển của standard audit:**
* Có thể enable ( các bản ghi được sinh ra và lưu trong audit trails) hoặc disable ( các bản ghi không được phát sinh) các các standard audit.
* Xóa một bản ghi trong audit trail để giải phóng vùng nhớ đồng thời giúp việc quản lý tối ưu hơn



* + 1. **Xem thông tin audit:**
* Xem thông tin audit thông qua view DBA\_AUDIT\_TRAIL



* Kết quả:

A picture containing text, crossword puzzle, receipt

Description automatically generated

* + 1. **Thực hành đồ án**
* Vì bảng bệnh nhân chứa thông tin nhạy cảm nên cần audit lại tất cả các hành động select, insert, update và delete cho tất cả các user( cả thành công và thất bại)



* Vì trong đơn thuốc có tính chất quan trọng cần được theo dõi nên cần audit lại các hành động như delete, update, insert( cả thành công và thất bại)



* Chấm công và tính lương nhân viên là những thông tin cần phải chính xác cần phải theo dõi các hành động trên 2 bảng này (ghi lại nhưng hoạt động thực hiện thành công)

Text

Description automatically generated with medium confidence

* Thực hiện audit trên các thao tác trên role để theo dõi các role bị delete, hay được create



* Thực hiện audit các thao tác tạo xóa các thủ tục



* Thực hiện giám sát đăng nhập



1. **Quản lý chính sách audit DBMS\_FGA**
   * 1. **Thêm một DBMS\_FGA policy**

Graphical user interface, text, application

Description automatically generated

* + 1. **Enable/disable DBMS\_FGA policy**
* Enable:

Text

Description automatically generated

* Disable:

Text

Description automatically generated

* + 1. **Drop DBMS\_FGA policy**

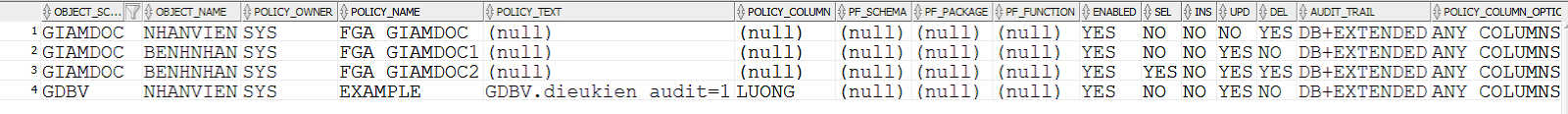
Text, letter

Description automatically generated

* + 1. **Xem dữ liệu audit**
* Xem các chính sách FGA đã cài đặt:



Kết quả:



* Xem dữ liệu audit được:



* + 1. **Thực hành đồ án**
* Chính sách 1: Ghi nhận lại các hành động thêm xóa sửa trên bảng Phiếu lương, mà người thực hiện không phải là nhân viên Kế toán:
* Vì theo chính sách bảo mật đã đề ra, chỉ có nhân viên Kế toán mới có quyền thêm, xóa, sửa trên bảng Phiếu lương. Vì vậy, nếu một user nào không phải là nhân viên kế toán mà lại thêm xóa sửa bảng Phiếu Lương được, thì ta audit lại

Text

Description automatically generated with medium confidence

*Hình CS1. Chính sách Audit trên bảng Phiếu lương*

* Chính sách 2: Ghi nhận lại những hành vi cập nhật cột lương trong bảng Nhân viên mà người thực hiện không phải là nhân viên thuộc đơn vị Quản lý tài nguyên nhân sự .
* Vì theo chính sách bảo mật đã đề ra: chỉ có nhân viên thuộc đơn vị Quản lý tài nguyên nhân sự mới được cập nhật cột lương của bảng Nhân viên. Vì vậy, nếu có user nào cập nhật được cột lương mà không phải là nhân viên Quản lý tài nguyên nhân sự thì hệ thống phải ghi nhận lại.

Graphical user interface, text, application, email

Description automatically generated

*Hình CS2. Chính sách Audit trên bảng Nhân viên*