**BỘ MÔN HỆ THỐNG THÔNG TIN – KHOA CÔNG NGHỆ THÔNG TIN**

**ĐẠI HỌC KHOA HỌC TỰ NHIÊN THÀNH PHỐ HỒ CHÍ MINH, ĐẠI HỌC QUỐC GIA TP HCM**

Nhóm thực hiện: Nhóm 16

GV phụ trách: Phạm Thị Bạch Huệ

Đồ án Thực hành môn học  - AN TOÀN & BẢO MẬT TRONG HỆ THỐNG THÔNG TIN

HỌC KỲ II – NĂM HỌC 2019-2020

**môn AN TOÀN & BẢO MẬT TrONG httt**

**BẢNG THÔNG TIN CHI TIẾT NHÓM**

|  |  |  |  |
| --- | --- | --- | --- |
| **Mã nhóm:** | 16 | | |
| **Số lượng:** | **4** | | |
| **MSSV** | **Họ tên** | **Email** | **Điện thoại** |
| 1712879 | Phan Văn Tuấn | 1712879@student.hcmus.edu.vn |  |
| 1712850 | Trần Trung | 1712850@student.hcmus.edu.vn |  |
| 1712841 | Phạm Văn Trình | 1712841@student.hcmus.edu.vn |  |
| 1712848 | Phạm Quốc Trung | 1712848@student.hcmus.edu.vn |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Bảng phân công & đánh giá hoàn thành công việc** | | | |
| **Công việc thực hiện** | **Người thực hiện** | **Mức độ hoàn thành** | **Đánh giá của nhóm** |
| Phân hệ 2 : Phân tích chính sách bảo mật ,tạo user & role,cài đặt cơ chế mã hóa dữ liệu,cài đặt VPD,cài đặt chức năng Login,cài đặt OLS,giao diện QL TNNS,giao diện QL Tài vụ,giao diện QL Chuyên môn | Phan Văn Tuấn | 100% | 9/10 |
| Phân hệ 2 : Thiết kế DB và sinh dữ liệu mẫu,giao diện Nhân viên phòng tài vụ, giao diện Bác sĩ, giao diện Nhân viên bộ phận bán thuốc, giao diện Nhân viên kế toán | Trần Trung | 100% | 9/10 |
| Phân hệ 1: Giao diện xem danh sách người dùng,thông tin quyền, tạo mới, xóa , chỉnh sửa user, role. Audit. | Phạm Văn Trình | 95% | 9/10 |
| Phân hệ 1:  Giao diện thực hiện cấp quyền, thu hồi và chỉnh sửa quyền,kiểm tra quyền vừa cấp. | Phạm Quốc Trung | 95% | 9/10 |

**YÊU CẦU ĐỒ ÁN- BÀI TẬP**

|  |  |
| --- | --- |
| **Loại bài tập** | **Lý thuyết 🗹 Thực hành 🗹 Đồ án Bài tập** |
| **Ngày bắt đầu** |  |
| **Ngày kết thúc** |  |

**MỤC LỤC**

[I. PHÂN HỆ 1: DÀNH CHO NGƯỜI QUẢN TRỊ CƠ SỞ DỮ LIỆU 3](#_Toc49753479)

[1.Xem danh sách đối tượng hiện có trên CSDL 3](#_Toc49753480)

[2. Thêm mới đối tượng 4](#_Toc49753481)

[3.Phân quyền user/sql. 6](#_Toc49753482)

[4. Chức năng ghi nhật ký hệ thống (chỉ yêu cầu thực hiện mức HQT CSDL Oracle): 8](#_Toc49753483)

[*a.Admin có quyền enable/ disable việc ghi nhật ký toàn hệ thống* 8](#_Toc49753484)

[*b.Ghi nhật khi của các hành động Logon, Logoff của user.*  Ta cài đặt như sau: 9](#_Toc49753485)

[*c.Ghi nhật kí hành động trên table*  10](#_Toc49753486)

[*d.Ghi nhật kí hành động trên views* 11](#_Toc49753487)

[II. PHÂN HỆ 2: QUẢN LÝ THÔNG TIN CỦA MỘT BỆNH VIỆN 11](#_Toc49753488)

[1.Tóm tắt danh sách các đối tượng trong hệ thống: 11](#_Toc49753489)

[2.Mô hình dữ liệu cho hệ thống 13](#_Toc49753490)

[3.Cơ chế bảo mật đã thực hiện 13](#_Toc49753491)

[4.Mã hóa dữ liệu 13](#_Toc49753492)

[5. Cơ chế OLS 14](#_Toc49753493)

[*a.Tạo chính sách OLS* *BEGIN* 14](#_Toc49753494)

[*b.Định nghĩa các thành phần sẽ tạo thành nhãn* 14](#_Toc49753495)

[*c.Gán chính sách OLS cho table* 15](#_Toc49753496)

[*d.Gán nhãn cho user* 16](#_Toc49753497)

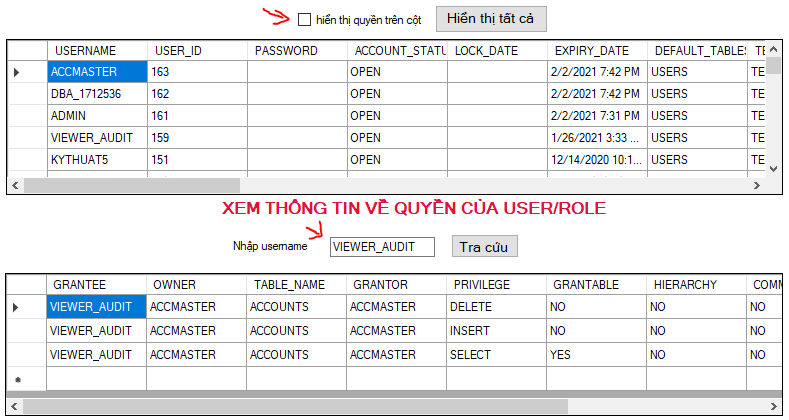
[*e.Hình ảnh minh họa:* 17](#_Toc49753498)

[6.Auditing 17](#_Toc49753499)

1. **PHÂN HỆ 1: DÀNH CHO NGƯỜI QUẢN TRỊ CƠ SỞ DỮ LIỆU**

## 1.Xem danh sách đối tượng hiện có trên CSDL

Giao diện xem danh sách user role trong hệ thống và quyền tương ứng.Nhập tên user vào ô tra cứu để tìm kiếm user và quyền.

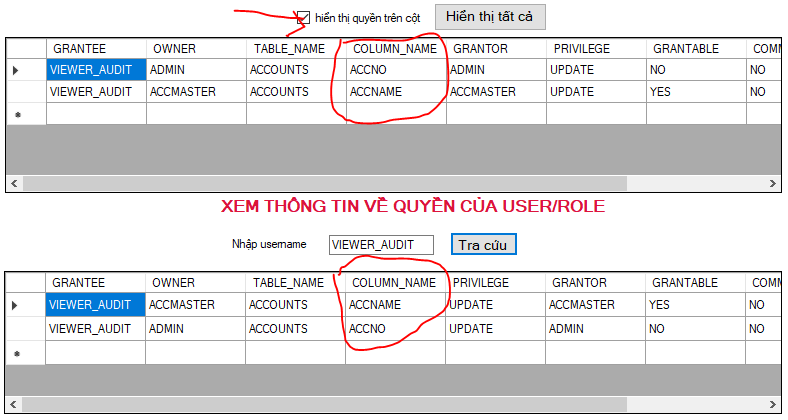


Nếu muốn xem các quyền được cấp trên cột, tick vào ô chọn hiển thị quyền trên cột.

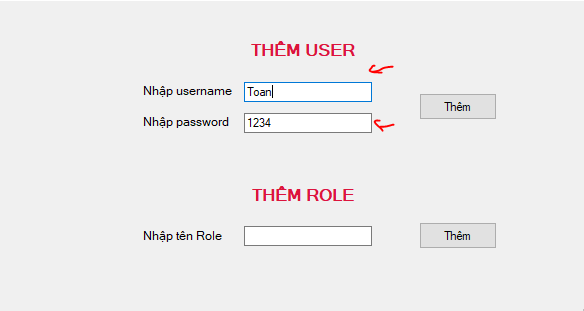
PLSQL:

xem tất cả quyền: select \* from DBA\_COL\_PRIVS WHERE GRANTEE <> 'IMP\_FULL\_DATABASE'

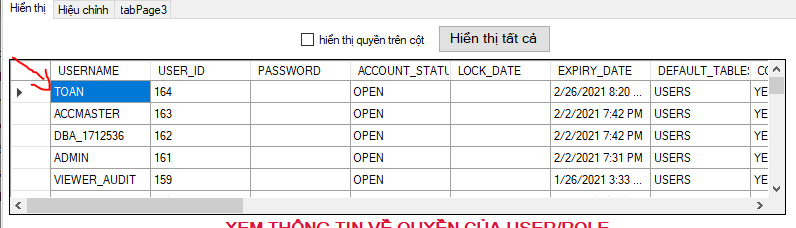
xem quyền cấp trên cột: SELECT\* FROM DBA\_USERS order by created DESC



## **2. Thêm mới đối tượng**



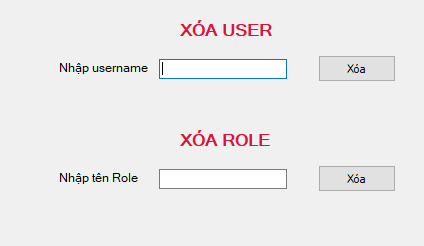
Kiểm tra lại thấy user vừa thêm.



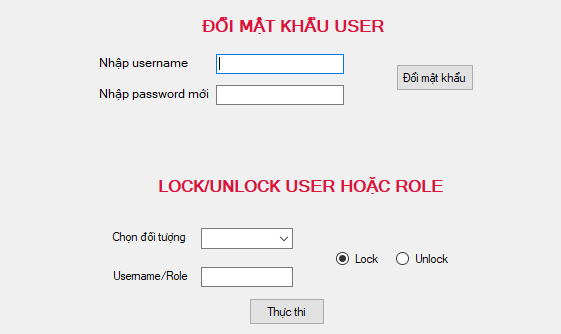
PLSQL:

CREATE USER {txtUsername.Text} IDENTIFIED BY {txtPassword.Text}

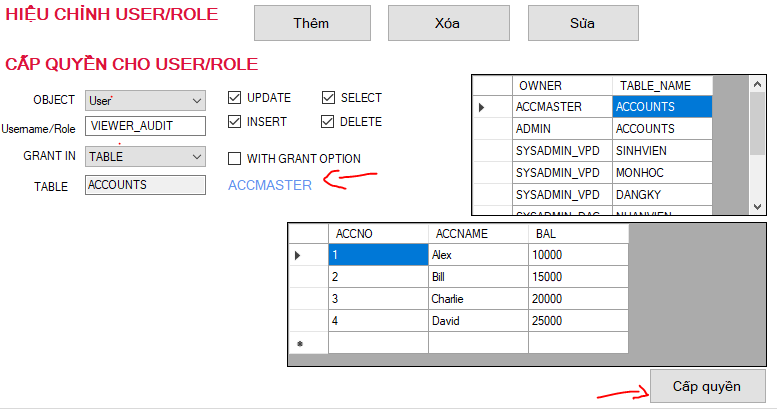
Xóa user/Role:



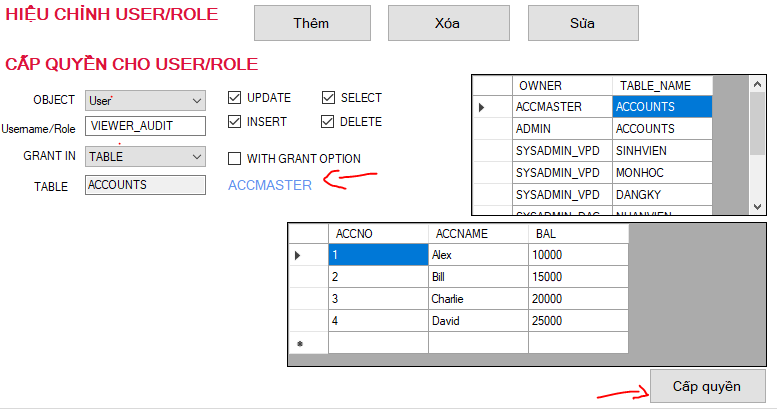
Sửa user/role: cho phép admin đổi mật khẩu user. Lock hoặc unlock user bất kì.Hoặc Lock tất cả Role.



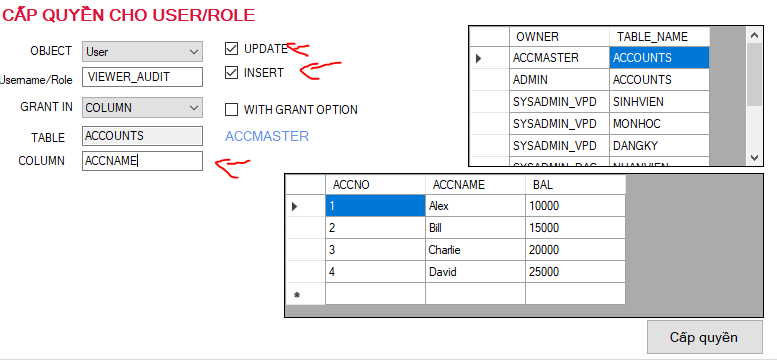
## **3.Phân quyền user/sql.**



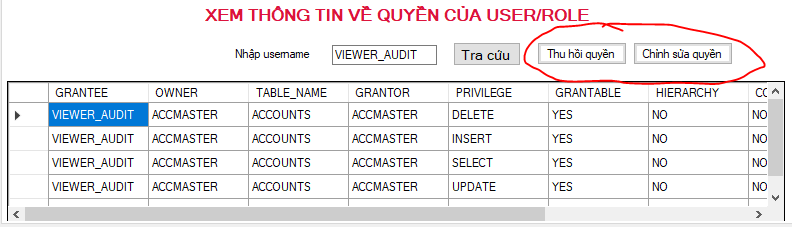
Cấp quyền cho user



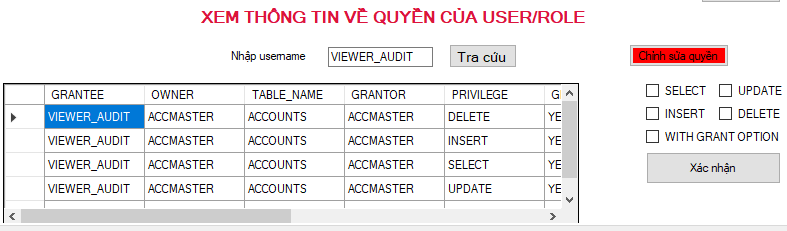
Cấp quyền trên cột cho Role/User:Chỉ được phép cấp quyền update và insert trên cột



Thu hồi quyền user hoặc role.Nhập tên role/user, chọn tra cứu, sau đó click vào dòng cần chỉnh hoặc thu hồi sẽ hiện ra button để thu hồi



Chỉnh sửa quyền:Click vào dòng cần chỉnh sửa sau đó chọn chỉnh sửa quyền sau đó xác nhận chỉnh sửa.



## **4. Chức năng ghi nhật ký hệ thống (chỉ yêu cầu thực hiện mức HQT CSDL Oracle):**

### *a.Admin có quyền enable/ disable việc ghi nhật ký toàn hệ thống*

Đầu tiên ta kiểm tra trạng thái Audit là đang bật hay tắt bằng câu lệnh

show parameter audit\_trail

**NONE:** auditing tắt

**DB,EXTENDED:** Auditingbật**,** (tất cả các nhật kí được lưu trong bảng(SYS.AUD$).

**XML, EXTENDED**- Auditingbật**,** (tất cả các nhật kí được lưu trong file dạng XML ).

**OS**- Auditingbật**,** (tất cả các nhật kí được lưu trong file hệ thống ).

* Để bật Audit ta cần thay trạng thái của biến audit\_trail qua câu query:

ALTER SYSTEM SET audit\_trail=db SCOPE=SPFILE;

* Ngược lại để tắt Audit ta thực hiện câu query

ALTER SYSTEM SET audit\_trail=NONE SCOPE=SPFILE;

### *b.Ghi nhật khi của các hành động Logon, Logoff của user.* Ta cài đặt như sau:

* Đầu tiên ta tạo 1 table chứa dữ liệu nhật kí

create table audit\_log(name varchar2(50), time date, action varchar2(50));

* Tiếp theo, tạo trigger để ghi lại hành động logon và logoff

--LOGON

create or replace trigger logon\_trig

after logon on database

begin

insert into audit\_log values (user, sysdate, 'LOGON');

commit;

end logon\_trig;

--LOGOFF

create or replace trigger logoff\_trig

before logoff on database

begin

insert into audit\_log values (user, sysdate, 'LOGOFF');

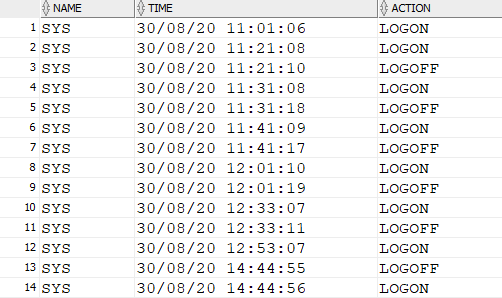
commit;

end logoff\_trig;

* Kiểm tra lại kết quả

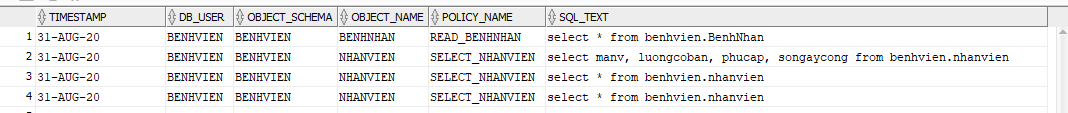
alter session set nls\_date\_format='dd/mm/yy hh24:mi:ss';

select \* from audit\_log;

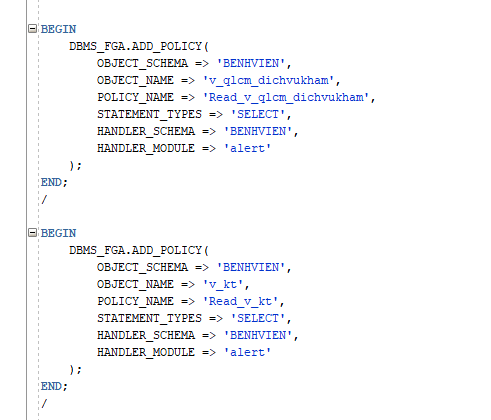


### *c.Ghi nhật kí hành động trên table*

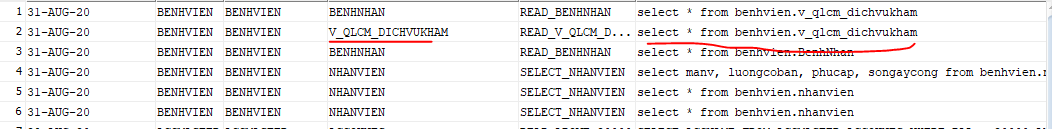
kết quả test:



### *d.Ghi nhật kí hành động trên views*



kết quả test:



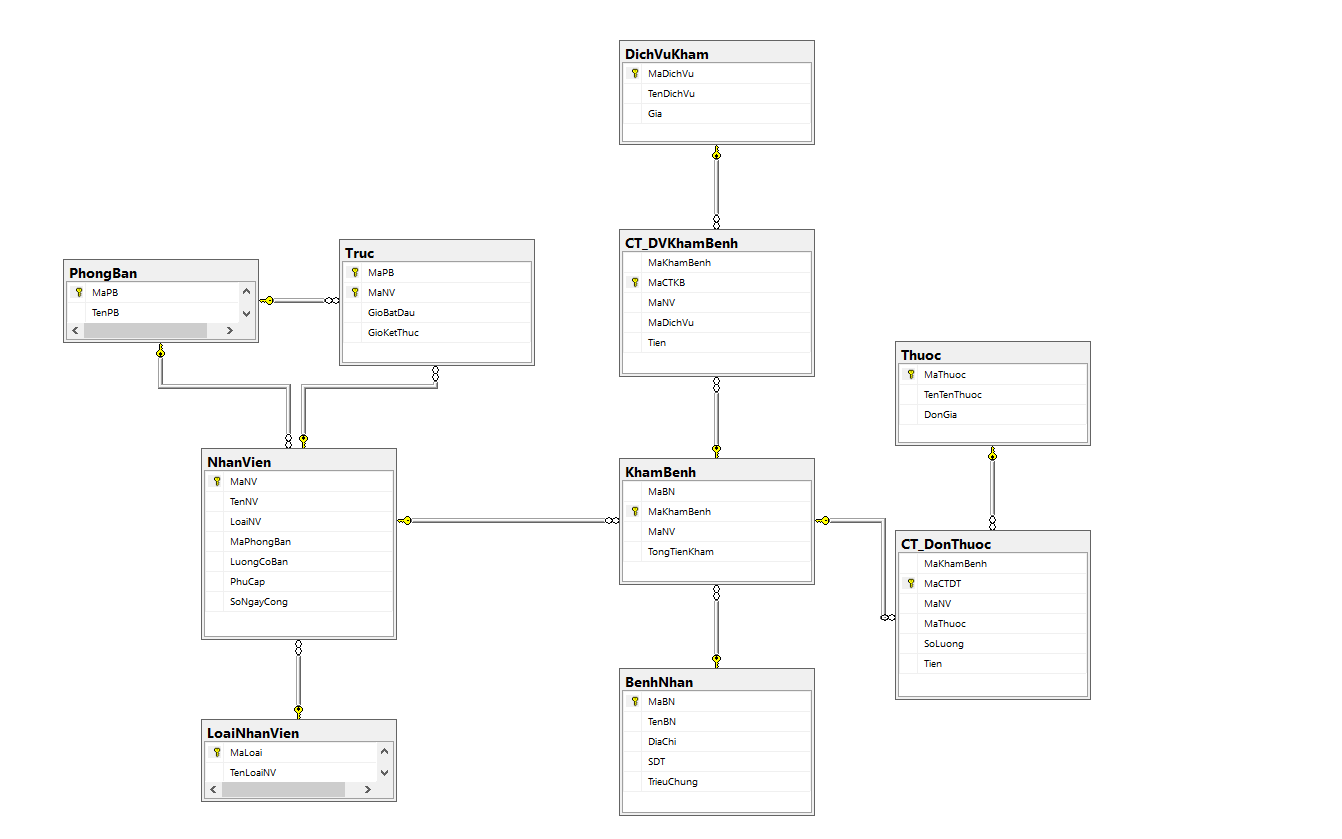
# PHÂN HỆ 2: QUẢN LÝ THÔNG TIN CỦA MỘT BỆNH VIỆN

## 1.Tóm tắt danh sách các đối tượng trong hệ thống:

1. Bộ phận quản lý
   1. nhóm quản lý tài nguyên và nhân sự
   2. nhóm quản lý tài vụ
   3. nhóm quản lý chuyên môn
2. Bộ phận tiếp tân và điều phối bệnh
3. Nhân viên phòng tài vụ
4. Bác sĩ
5. Nhân viên bộ phận bán thuốc:
6. Nhân viên kế toán:

|  |  |
| --- | --- |
| **nhóm/ bộ phận** | **mô tả** |
| nhóm quản lý tài vụ | Nhập mới chỉnh sửa các thông tin liên quan đơn giá các loại dịch vụ khám bệnh, đơn giá thuốc  Những thông tin khác được quyền xem tất cả nhưng không được phép sửa. |
| nhóm quản lý tài nguyên nhân sự | Chỉ được thêm, xóa, sửa các thông tin trong cách danh mục như: phòng ban, bác sĩ, nhân viên trong từng phòng ban, bác sĩ nào trực phòng nào vào thời gian nào, …  và được xem tất cả các thông tin khác kể cả thông tin nhân viên kế toán tạo ra nhưng không được quyền sửa |
| Nhóm quản lý chuyên môn | xem tất cả thông tin trong đó có thông tin điều trị bệnh của các bác sĩ  không được chỉnh sửa bất cứ thông tin nào. |
| Bộ phận tiếp tân và điều phối bệnh | Có quyền thêm, xóa, sửa, tìm kiếm thông tin bệnh nhân  nhưng không thể xem các thông tin liên quan đến số tiền cho từng thủ tục khám, xét nghiệm hoặc chụp hình hoặc thông tin thuốc điều trị bệnh cho bệnh nhân. |
| Nhân viên phòng tài vụ | Chỉ được cập nhật số tiền phải trả cho từng chi tiết khám trị mà không được chỉnh sửa bất cứ thông tin gì.  nhìn thấy các thủ tục mà bác sĩ yêu cầu bệnh nhân phải làm khi điều trị bệnh  thông tin mà bộ phận điều phối bệnh đã điều phối và tính tiền. |
| Bác sĩ | Thêm hoặc sửa thông tin liên quan đến việc điều trị bệnh ,các loại thuốc phải dùng, liều dùng  không được xem hoặc chỉnh sửa thông tin khác của những bệnh nhân do bác sĩ khác  và những thông tin khác trong hệ thống |
| Nhân viên bộ phận bán thuốc: | nhìn thấy toa thuốc  để tính tiền thuốc cho bệnh nhân  và tính tiền  không thể xem được bệnh nhân bệnh  gì hay bất cứ thông tin gì khác. |
| Nhân viên kế toán: | tính lương cho các bác sĩ và các nhân viên khác  không nhìn thấy bất cứ thông tin gì quá trình điều trị bệnh cho bệnh nhân |

## 2.Mô hình dữ liệu cho hệ thống

****

## 3.Cơ chế bảo mật đã thực hiện

1. Định danh và xác thực bằng username & password
2. DAC: cấp quyền trên view và sử dụng grant cấp quyền
3. RBAC: Tạo các role cho từng nhóm/bộ phận
4. VPD: điều khiển truy cập dựa trên nội dung dữ liệu
5. Auditing: giám sát hành vi người dùng

## 4.Mã hóa dữ liệu

**Phương pháp mã hóa**:

* sử dụng bộ thuật toán mã hóa DES\_CBC\_PKCS5
* sử dụng thư viện: DBMS\_CRYPTO

**Mục đích**: những đối tượng dữ liệu rất “nhạy cảm” hạn chế người dùng truy xuất vào

**Các đối tượng cần mã hóa**:

* Bảng nhân viên (lương cơ bản, phụ cấp, ngày công)
* Bảng bệnh nhân (triệu chứng)
* Bảng CT đơn thuốc (mã thuốc, tiền)
* Bảng CT DV khám bệnh (mã dịch vụ, tiền)
* Bảng  Khám bệnh(Mã BN, Tổng Tiền Khám)

**Phương pháp quản lý khóa**: lưu khóa trong CSDL

sử dụng OLS để bảo vệ, gán label mức cao nhất cho table đảm bảo tuyệt đối

## 5. Cơ chế OLS

### *a.Tạo chính sách OLS* *BEGIN*

*sa\_sysdba.create\_policy*

*(policy\_name => ‘CS\_OLS’,*

*column\_name => 'COT\_OLS');*

*END;*

### *b.Định nghĩa các thành phần sẽ tạo thành nhãn*

**Tạo group:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Group num** | **Parent\_name** | **Long name** | **Short name** |
| **1** | null | Bệnh Viện | BV |
| **100** | BV | Miền Bắc | MB |
| **110** | BV | Miền Trung | MT |
| **120** | BV | Miền Nam | MN |
|  |  |  |  |

**Tạo compartment:**

|  |  |  |
| --- | --- | --- |
| **Dạng số** | **Tên dài** | **Tên ngắn** |
| **1000** | Nhóm quản lý tài nguyên nhân sự | QLTNNS |
| **900** | Nhóm quản lý tài vụ | QLTV |
| **800** | Nhóm quản lý chuyên môn | QLCM |
| **700** | Bộ Phận TT & ĐP | TTDP |
| **600** | Phòng Tài Vụ | PTV |
| **500** | Nhóm Bác Sĩ | NBS |
| **400** | Bộ Phận Bán Thuốc | BPBT |
| **300** | Bộ Phận Kế Toán | BPKT |

**Tạo level:**

|  |  |  |
| --- | --- | --- |
| **Dạng số** | **Tên dài** | **Tên ngắn** |
| 9000 | Giám Đốc | EXEC |
| 8000 | Quản Lý | MGR |
| 7000 | Nhân Viên | EMP |

**Định nghĩa các nhãn**

|  |  |
| --- | --- |
| **Label tag** | **Label value** |
| **300** | EMP: QLTNNS: MN |
| **310** | EMP: QLTV: MN |
| **320** | EMP: QLCM : MN |
| **330** | EMP: TTDP: MN |
| **340** | EMP: PTV: MN |
| **350** | EMP: NBS: MN |
| **360** | EMP: BPBT: MN |
| **370** | EMP: BPKT: MN |
| **375** | MGR: QLTNNS: MN |
| **380** | MGR: QLTV: MN |
| **390** | MGR: QLCM : MN |
| **400** | MGR: TTDP: MN |
| **410** | MGR: PTV: MN |
| **420** | MGR: PBS: MN |
| **430** | MGR: BPBT: MN |
| **440** | MGR: BPKT: MN |
| **450** | EXEC: QLTNNS, QLTV, QLCM, TTDP, PTV, PBS, BPBT, BPKT: MN |

### *c.Gán chính sách OLS cho table*

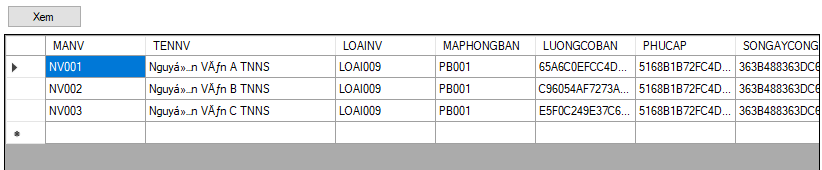
|  |  |
| --- | --- |
| **Table** | **Label** |
| **Nhân Viên** | tùy vào vai trò của nhân viên sẽ có label tương ứng |
| **KEYEN** | EXEC:BPKT,BPBT,NBS,PTV,TTDP,QLCM,QLTV,QLTNNS:MN |

### *d.Gán nhãn cho user*

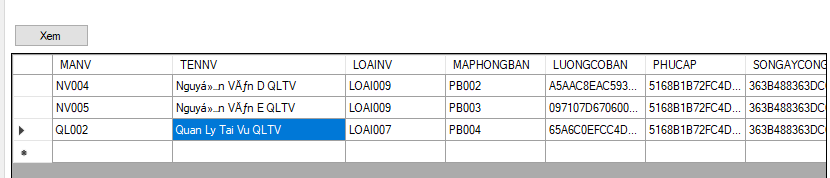
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Username** | **Max\_read\_label** | **Max\_write\_label** | **Def\_label** | **Row\_label** |
| **GD001** | EXEC: BPKT,BPBT,NBS,PTV,TTDP,QLCM,QLTV,QLTNNS: MN | EXEC: BPKT,BPBT,NBS,PTV,TTDP,QLCM,QLTV,QLTNNS:MN | EXEC: BPKT,BPBT,NBS,PTV,TTDP,QLCM,QLTV,QLTNNS: MN | EXEC: BPKT,BPBT,NBS,PTV,TTDP,QLCM,QLTV,QLTNNS: MN |
| **NV001** | EMP:QLTNNS:MN | EMP:QLTNNS:MN | EMP:QLTNNS:MN | EMP:QLTNNS:MN |
| **NV002** | EMP:QLTNNS:MN | EMP:QLTNNS:MN | EMP:QLTNNS:MN | EMP:QLTNNS:MN |
| **NV003** | EMP:QLTNNS:MN | EMP:QLTNNS:MN | EMP:QLTNNS:MN | EMP:QLTNNS:MN |
| **NV004** | EMP:QLTV:MN | EMP:QLTV:MN | EMP:QLTV:MN | EMP:QLTV:MN |
| **QL001** | MGR:QLTNNS:MN | MGR:QLTNNS:MN | MGR:QLTNNS:MN | MGR:QLTNNS:MN |
| **QL002** | MGR:QLTV:MN | MGR:QLTV:MN | MGR:QLTV:MN | MGR:QLTV:MN |
| **QL003** | MGR:QLCM:MN | MGR:QLCM:MN | MGR:QLCM:MN | MGR:QLCM:MN |
| **QL004** | MGR:TTDP:MN | MGR:TTDP:MN | MGR:TTDP:MN | MGR:TTDP:MN |
| **QL005** | MGR:PTV:MN | MGR:PTV:MN | MGR:PTV:MN | MGR:PTV:MN |
| **QL006** | MGR:NBS:MN | MGR:NBS:MN | MGR:NBS:MN | MGR:NBS:MN |
| **QL007** | MGR:BPBT:MN | MGR:BPBT:MN | MGR:BPBT:MN | MGR:BPBT:MN |
| **QL008** | MGR:BPKT:MN | MGR:BPKT:MN | MGR:BPKT:MN | MGR:BPKT:MN |

### *e.Hình ảnh minh họa:*

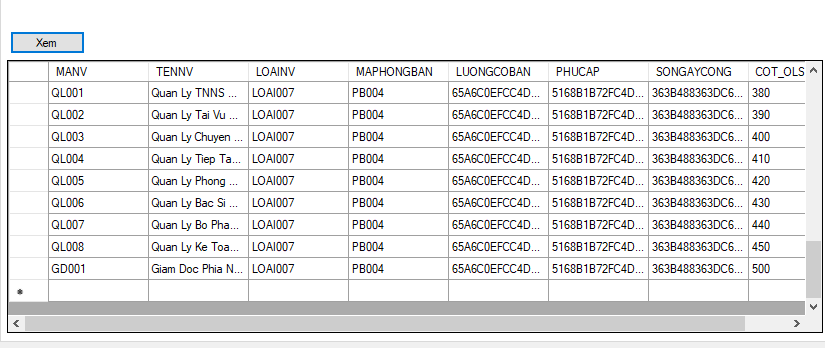
Khi login bằng user **nhân viên** thuộc nhóm “”Quản Lý Tài Nguyên Nhân Sự” chỉ xem được danh sách các nhân viên cùng phòng



Khi login bằng user **quản lý** thuộc nhóm “”Quản Lý Tài Vụ” xem được danh sách các nhân viên cùng phòng và thông tin quản lý



Khi login bằng user **giám đốc miền nam** xem được danh sách các nhân viên ở miền nam



## 6.Auditing

**Mục đích:** giám sát hành vi người dùng khi thao tác với dữ liệu “nhạy cảm” trong hệ thống

**Các hành vi cần phải giám sát:**

* Đọc thông tin lương cơ bản của nhân viên
* Đọc thông tin của bệnh nhân(triệu chứng)
* Đọc thông tin tính lương của nhân viên kế toán