**PHẦN 1: HỆ THỐNG DÀNH CHO NGƯỜI QUẢN TRỊ BẢO MẬT**

* 1. Nhận diện người quản trị và hiển thị màn hình cho người quản trị:
  2. Xem danh sách các đối tượng trên CSDL (role, user, view, table…).
  3. Thêm mới các đối tượng (role, user, view, table,…).
  4. Phần quyền và lấy lại quyền của User/Role.
  5. Xem quyền của một chủ thể cụ thể.
  6. Các kiến thức cần có để thực hiện các yêu cầu trên.

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

+ Xem danh sách user: select username from dba\_users;

+ Xem danh sách role: select role from dba\_roles;

+ Xem danh sách table: select table\_name from user\_tables;

+ Xem danh sách view: select view\_name from user\_views;

1. Xóa đối tượng

+ Xóa user: drop user username cascade;

+ Xóa role: drop role rolename;

+ Xóa table: drop table table\_name cascade constraints;

1. Thêm đối tượng

+ Thêm user: create user username identified by password;

+ Thêm role: create role role\_name;

1. Phân quyền và lấy lại quyền
   * 1. Phân quyền

+ Cấp quyền tạo session: grant create session to username;

+ Cấp quyền tạo table: grant create table to username;

+ Cấp quyền tạo view: grant create view to username;

+ Cấp quyền DBA: grant dba to username;

+ Cấp quyền trên một object cụ thể:

Grant select || insert || update || delete on object to subject

Object: là table hoặc view

Subect: là user hoặc role

+ Cấp quyền execute procedure cho người dùng: grant execute on procedure to subject;

Procedure: tên procedure

Subject: user hoặc role

* + 1. Lấy lại quyền

+ Lấy quyền tạo session: revoke create session from username;

+ Lấy lại quyền tạo table: revoke create table from username;

+ Lấy lại quyền tạo view: revoke create view from username;

+ Lấy lại quyền DBA: revoke dba from username;

+ Lấy lại quyền trên object cụ thể

Revoke select || insert || update || delete on object from subject

Object: là table hoặc view

Subect: là user hoặc role

1. Xem quyền của một chủ thể cụ thể

+ Xem quyền của một user: select \* from USER\_TAB\_PRIVS where grantee = username;

+ Xem quyền của một role: select \* from ROLE\_TAB\_PRIVS where role = rolename;

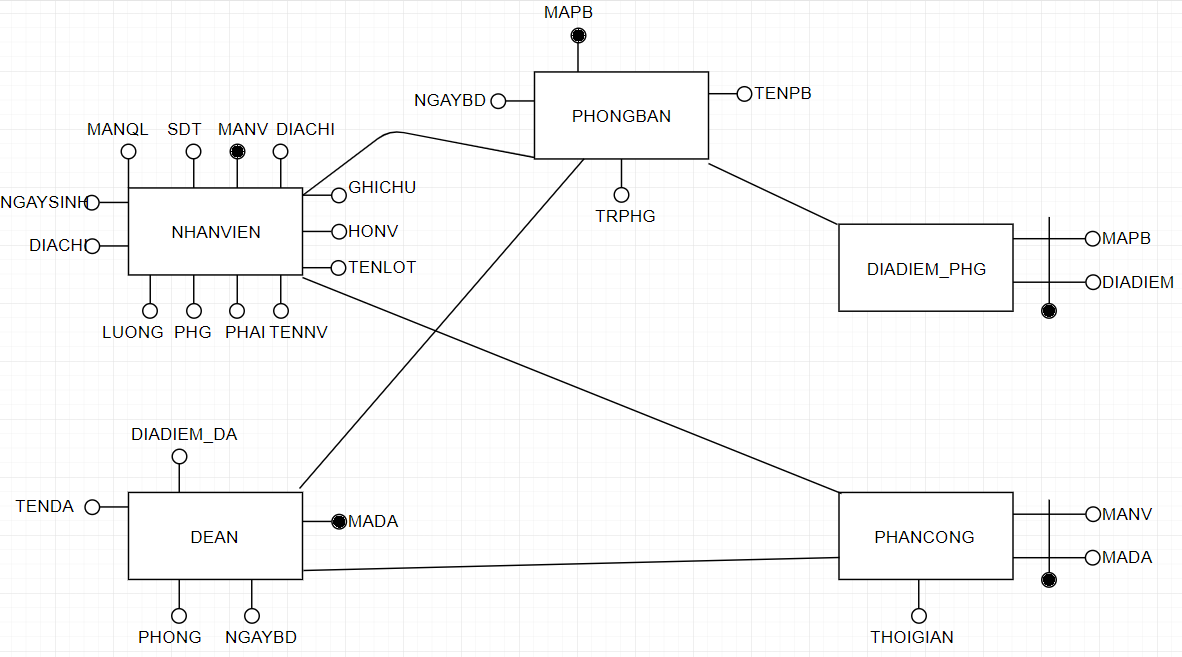
**PHẦN 2**: **HIỆN THỰC CÁC CHÍNH SÁCH BẢO MẬT**

1. Lược đồ cơ sở dữ liệu được quan hệ được dùng:

* NHANVIEN (MANV, HONV, TENLOT, TENNV, PHAI, LUONG, DIACHI, NGAYSINH, MANQL, PHG, GHICHU)
* PHONGBAN (MAPB, TENPB, TRPHG, NGAYBD)
* DIADIEM\_PHG (MAPB, DIADIEM)
* DEAN (MADA, TENDA, NGAYBD, PHONG, DIADIEM\_DA)
* **PHANCONG** (MANV, MADA, THOIGIAN)

Trong đó: gạch chân nét liền là “khóa chính” và gạch chân nét đứt là “khóa ngoại”.

**Lược đồ ER:**

****

1. Các chính sách bảo mật phân loại:
2. DAC
   1. **Chỉ có giám đốc, các trưởng phòng, những nhân viên Phòng Thực hiện đề án, nhân viên Phòng Kinh doanh và Phòng Kế hoạch mới có thể xem thông tin về đề án và việc phân công vào các đề án.**
      1. Mô tả:

* Các loại nhân viên: Giám đốc, trưởng phòng các phòng ban, nhân viên các phòng: Thực hiện đề án, kế hoạch, kinh doanh.
* Các trường được truy suất: bảng đề án, nhân viên tham gia đề án, phòng ban thực hiện, thời gian thực hiện.
  + 1. Thực hiện:

1. Tạo các hàm sau để lấy những nhân viên theo chính sách trên và cấp quyền đó cho Role phù hợp, bao gồm các hàm:

* Lấy nhân viên là giám đốc.
* Lấy nhân viên là trưởng phòng của các phòng ban.
* Lấy những nhân viên thuộc các phòng: thực hiện đề án, phòng kế hoạch, phòng kinh doanh.

1. Tạo View để xem các trường của đề án và phân công đề án.
2. Cấp View đó cho các Role.
   1. Những nhân viên Phòng Kế hoạch mới được thêm, xóa, sửa dữ liệu liên quan các đề án.
      1. Mô tả:

* Các loại nhân viên: nhân viên phòng kế hoạch.
* Các trường truy suất: dữ liệu liên quan đến đề án.
  + 1. Thực hiện:

1. Tạo các procedure

* Create Or Replace Procedure PKH\_UPDATE\_DEAN
* Create Or Replace Procedure PKH\_INSERT\_DEAN

1. Cấp quyền “execute” đến role nhân viên phòng kế hoạch
2. RBAC
   1. Các role được xây dựng và các quyền trên được cấp trên Role:

* p\_GIAMDOC: VIEW\_DEAN
* p\_TRUONGPHONG: VIEW\_DEAN
* p\_NHANVIEN\_PKH: VIEW\_DEAN, quyền execute Procedure PKH\_UPDATE\_DEAN, quyền execute Procedure PKH\_INSERT\_DEAN
* p\_NHANVIEN\_PNS
* p\_NHANVIEN\_PKD: VIEW\_DEAN
* p\_NHANVIEN\_PTHDA: VIEW\_DEAN
  1. Các “View" được xây dựng lên để phục vụ các yêu cầu truy suất.
* VIEW\_DEAN.

2.3 Các “USER” được lấy chính là “MANV” của các nhân viên.

Các “USER” được thừa hưởng các Role nêu trên:

* p\_GIAMDOC: nhân viên là giám đốc.
* p\_TRUONGPHONG: trường phòng các phòng ban.
* p\_ NHANVIEN\_PKH: nhân viên phòng kế hoạch.
* p\_NHANVIEN\_PNS: phân viên phòng nhân sự.
* p\_NHANVIEN\_PKD: nhân viên phòng kinh doanh.
* p\_NHANVIEN\_PTHDA: nhân viên phòng thực hiện đề án.

1. VPD
   1. Nhânviên chỉđược xem các trường lương, phụcấp của chính nhân viên đó.
      1. Mô tả:

+ Khi nhân viên login vào tài khoản của mình, nhân viên thực hiện xem trên bảng nhân viên, câu truy vấn sẽ trả về các trường lương và phụ cấp của chính nhân viên đang “login” mà không được phép xem các trường lương và phụ cấp của bất kì nhân viên nào khác cả.

* + 1. Thực hiện:

+ Tạo một function trả về nhân viên đang ‘login’

+ Gắn hàm chính sách chỉ nhân viên được phép xem lương của mình lên bảng nhân viên.

* 1. Trưởng phòng chỉ được phép xem thông tin nhân viên của phòng ban mình.
     1. Mô tả:
     2. Thực hiện:

+ Gắn hàm chính sách vào bảng nhân viên để chi trưởng phòng mới được phép xem lương của bản thân mình.

1. Mã hóa
   1. Mã hóa thông tin lương của các nhân viên
   2. Mã hóa thông tin mật khẩu.
2. Audit

Ghi lại thông tin “insert” và “update” của nhân viên khi nhân viên đó thực hiện, lưu lại hành dộng của nhân viên đó.