**Bài tập lớn**

**BẢO MẬT CƠ SỞ DỮ LIỆU**

**Quy định chung:**

* Ngôn ngữ lập trình sử dụng trong các bài tập là tùy chọn (C, C++,VB , Java, .NET,…)
* Hệ quản trị cơ sở dữ liệu: Oracle
* Các framework mới (MERN, Python, PHP…)
* Nhóm từ **2-3** sinh viên.

# ĐỀ 1: Xây dựng ứng dụng web có chức năng quản lý người dùng

## Mô tả

Xây dựng 1 ứng dụng web theo mô hình 3 lớp (3-layer model), gồm:

* ***Presentation layer***: phục vụ việc nhận request từ phía client, thay mặt client gửi request cho các lớp bên dưới và hiển thị các kết quả trả về cho client. Áp dụng mô hình passive MVP (Model-View-Presenter) .
* ***Business layer***: chứa các thành phần xử lý các chức năng chính.
* ***Data layer***: truy xuất dữ liệu từ CSDL. Dùng Oracle DBMS.

User

Presentation Layer

Business Layer

Data Layer

CSDL

## Yêu cầu

Hiện thực các chức năng để quản lý user cho ứng dụng đó, cụ thể:

* Chức năng log in (áp dụng 1 phương pháp mã hóa cho việc lưu password).
* Tạo/xóa/thay đổi user :

Các thông tin mà 1 user account có thể được thiết lập (khi tạo mới hoặc khi thay đổi user) gồm :

* + - Username, Password
    - Default\_tablespace, Temporary\_tablespace (SV tạo sẵn trên CSDL Oracle một số tablespace để admin có thể gán cho các user chứ không cần hiện thực chức năng tạo/xóa tablespace).
    - Quota
    - Account status (lock/unclock)
    - Profile
    - Role
* Tạo/xóa/thay đổi profile (khái niệm profile trong CSDL Oracle) :

Ứng dụng cần cho phép gán/thay đổi các resource sau của profile (theo 3 loại là Unlimited, Default, một số cụ thể do người dùng gán):

* + - Sessions\_per\_user
    - Connect\_time
    - Idle\_time

Ứng dụng không cần thiết quản lý các giới hạn resource này của các user khi user đó log in vào hệ thống mà chỉ cần cho phép thiết lập giá trị cho các giới hạn resource này.

* Tạo/xóa/thay đổi role:

Cho phép thiết lập các thông tin sau khi tạo/thay đổi role:

* + - Role có password hay không
    - Nếu role có password, cho phép thay đổi password của role
* Gán/thu hồi quyền/role trên user/role:

Cho phép gán các quyền sau cho user/role:

* + - Quyền hệ thống:
* CREATE PROFILE\*, ALTER PROFILE\*, DROP PROFILE\*
* CREATE ROLE\*, ALTER ANY ROLE\*, DROP ANY ROLE\*, GRANT ANY ROLE\*
* CREATE SESSION\*
* CREATE ANY TABLE, ALTER ANY TABLE, DROP ANY TABLE, SELECT ANY TABLE\*, DELETE ANY TABLE, INSERT ANY TABLE, UPDATE ANY TABLE
* CREATE TABLE
* CREATE USER\*, ALTER USER\*, DROP USER\*
  + - Quyền đối tượng (object privilege) trên một table cụ thể:

SELECT\*, INSERT, DELETE

* + - Quyền đối tượng (object privilege) trên một column cụ thể:

SELECT\*, INSERT

Người gán quyền/role có thể thiết lập thêm tùy chọn là cho phép người được gán quyền/role được phép gán quyền/role đó cho những user/role khác (lưu ý các quyền trên đối tượng có hạn chế đối với tùy chọn này.Các SV tự tìm hiểu đó là hạn chế gì).

Các lệnh được đánh dấu \* ở bên trên là những lệnh mà ứng dụng cần kiểm tra xem một user có quyền đó không trước khi cho phép user đó thực hiện những hành động cần có quyền đó.

* Các table :

Ứng dụng cần truy xuất các bảng hệ thống của Oracle để lấy các thông tin cần thiết và cho hiển thị các thông tin đó theo dạng bảng cho admin xem khi cần thiết:

* + - Table quản lý quyền : liệt kê tất cả các quyền và user nào đang được cấp những quyền nào.
    - Table quản lý role : liệt kê tất cả các role, những quyền của role đó và user nào đang được gán role đó.
    - Table quản lý profile : liệt kê tất cả các profile, các resource thuộc từng profile và các user đang được gán profile đó.
    - Table quản lý thông tin các user :

Riêng đối với loại thông tin này, mọi user đều có quyền xem những thông tin account của user đó (riêng admin có quyền xem thông tin của tất cả các user):

* Username
* Account\_status,Lock\_date, Created\_date
* Default\_tablespace,Temporary\_tablespace, Quota
* Profile : lưu ý đây là khái niệm profile trong Oracle
* Role (cho thấy user được cấp role nào, user đó có được gán role đó cho user khác hay không)
* Privilege (cho thấy user có những quyền nào, được cấp trực tiếp hay thông qua role, user có được cấp quyền đó cho user khác hay không).

Ngoài những thông tin trên, SV nên tạo 1 table để quản lý những thông tin bình thường của user như họ tên, địa chỉ, số điện thoại, email,v.v... Table này do SV tự thiết kế. Chủ yếu để có thể cho demo chức năng gán quyền trên đối tượng của ứng dụng.

# ĐỀ 2: Xây dựng ứng dụng Windows có chức năng quản lý người dùng

## Mô tả

Xây dựng 1 ứng dụng windows theo mô hình 3 lớp (3-layer model), gồm:

* ***Presentation layer***: xử lý phần hiển thị, giao diện. Áp dụng mô hình passive MVP.
* ***Business layer***: chứa các thành phần xử lý các chức năng chính.
  + - ***Data layer***: truy xuất dữ liệu từ CSDL. Dùng Oracle DBMS.

User

Presentation Layer

Business Layer

Data Layer

CSDL

## Yêu cầu

Hiện thực các chức năng để quản lý user cho ứng dụng đó, cụ thể:

* Chức năng log in (áp dụng 1 phương pháp mã hóa cho việc lưu password).
* Tạo/xóa/thay đổi user :

Các thông tin mà 1 user account có thể được thiết lập (khi tạo mới hoặc khi thay đổi user) gồm :

* + - Username,Password
    - Default\_tablespace, Temporary\_tablespace (SV tạo sẵn trên CSDL Oracle một số tablespace để admin có thể gán cho các user chứ không cần hiện thực chức năng tạo/xóa tablespace).
    - Quota
    - Account status (lock/unclock)
    - Profile
    - Role
* Tạo/xóa/thay đổi profile (khái niệm profile trong CSDL Oracle) :

Ứng dụng cần cho phép gán/thay đổi các resource sau của profile (theo 3 loại là Unlimited, Default, một số cụ thể do người dùng gán):

* + - Sessions\_per\_user
    - Connect\_time
    - Idle\_time

Ứng dụng không cần thiết quản lý các giới hạn resource này của các user khi user đó log in vào hệ thống mà chỉ cần cho phép thiết lập giá trị cho các giới hạn resource này.

* Tạo/xóa/thay đổi role:

Cho phép thiết lập các thông tin sau khi tạo/thay đổi role:

* + - Role có password hay không
    - Nếu role có password, cho phép thay đổi password của role
* Gán/thu hồi quyền/role trên user/role:

Cho phép gán các quyền sau cho user/role:

* + - Quyền hệ thống:
* CREATE PROFILE\*, ALTER PROFILE\*, DROP PROFILE\*
* CREATE ROLE\*, ALTER ANY ROLE\*, DROP ANY ROLE\*, GRANT ANY ROLE\*
* CREATE SESSION\*
* CREATE ANY TABLE, ALTER ANY TABLE, DROP ANY TABLE, SELECT ANY TABLE\*, DELETE ANY TABLE, INSERT ANY TABLE, UPDATE ANY TABLE
* CREATE TABLE
* CREATE USER\*, ALTER USER\*, DROP USER\*
  + - Quyền đối tượng (object privilege) trên một table cụ thể:

SELECT\*, INSERT, DELETE

* + - Quyền đối tượng (object privilege) trên một column cụ thể:

SELECT\*, INSERT

Người gán quyền/role có thể thiết lập thêm tùy chọn là cho phép người được gán quyền/role được phép gán quyền/role đó cho những user/role khác (lưu ý các quyền trên đối tượng có hạn chế đối với tùy chọn này.Các SV tự tìm hiểu đó là hạn chế gì).

Các lệnh được đánh dầu \* ở bên trên là những lệnh mà ứng dụng cần kiểm tra xem một user có quyền đó không trước khi cho phép user đó thực hiện những hành động cần có quyền đó.

* Các table :

Ứng dụng cần truy xuất các bảng hệ thống của Oracle để lấy các thông tin cần thiết và cho hiển thị các thông tin đó theo dạng bảng cho admin xem khi cần thiết:

* + - Table quản lý quyền : liệt kê tất cả các quyền và user nào đang được cấp những quyền nào.
    - Table quản lý role : liệt kê tất cả các role, những quyền của role đó và user nào đang được gán role đó.
    - Table quản lý profile : liệt kê tất cả các profile, các resource thuộc từng profile và các user đang được gán profile đó.
    - Table quản lý thông tin các user :

Riêng đối với loại thông tin này, mọi user đều có quyền xem những thông tin account của user đó (riêng admin có quyền xem thông tin của tất cả các user):

* Username
* Account\_status, Lock\_date, Created\_date
* Default\_tablespace,Temporary\_tablespace, Quota
* Profile : lưu ý đây là khái niệm profile trong Oracle
* Role (cho thấy user được cấp role nào, user đó có được gán role đó cho user khác hay không)
* Privilege (cho thấy user có những quyền nào, được cấp trực tiếp hay thông qua role, user có được cấp quyền đó cho user khác hay không)

Ngoài những thông tin trên, SV nên tạo 1 table để quản lý những thông tin bình thường của user như họ tên, địa chỉ, số điện thoại, email,v.v... Table này do SV tự thiết kế. Chủ yếu để có thể cho demo chức năng gán quyền trên đối tượng của ứng dụng.

# ĐỀ 3: Xây dựng một ứng dụng website cho quy trình cấp hộ chiếu lần đầu

## Mô tả chung quy trình cấp hộ chiếu lần đầu

Thông tin để người sử dụng đăng ký cấp hộ chiếu bao gồm (Họ và tên, địa chỉ thường trú, phái, CMND, điện thoại, email). Thông tin này sẽ được người đăng ký điền vào form online, nộp cho bộ phận xác thực **(XT)** và được lưu vào **Passport** data. Bộ phận này sau khi đối chiếu và kiểm chứng thông tin như CMND, hộ khẩu, …(giả sử các thông tin liên quan đến người đăng ký dùng để đối chiếu này được lưu trữ trong một database chung gọi là **Resident** Data) sẽ gửi các yêu cầu đăng ký này cho bộ phận xét duyệt **(XD)**. Các yêu cầu đăng ký sau khi được phê duyệt sẽ được gửi đến bộ phận lưu trữ **(LT)** và thông báo kết quả cho người đăng ký. Song song đó bộ phận giám sát **(GS)** chịu trách nhiệm theo dõi và giám sát các hoạt động trên.

* [XT] được quyền xem thông tin từ form đăng ký và thông tin liên quan đến người đăng ký (Resident Database)
* [XD] có quyền xem tất cả các thông tin quy định cấp hộ chiếu và chỉ được xem thông tin trên form đăng ký. Không được xem thông tin trong Resident Database.
* [LT] chỉ được xem các thông tin được phê duyệt (đồng ý hay không đồng ý cấp hộ chiếu) nhưng không xem được thông tin cá nhân và các dữ liệu liên quan khác.
* [GS] giám sát tất cả các hoạt động của các user thuộc các nhóm: [XT], [XD], [LT] từ khi gửi yêu cầu cấp hộ chiếu đến khi nhận kết quả.

## Ghi chú

* Dữ liệu mẫu cho quy trình này SV tự thiết kế và nộp kèm theo kết quả xây dựng được.
* SV phải sử dụng các kỹ thuật bảo mật trong nội dung thực hành hoặc là các công nghệ khác liên quan đến bảo mật cơ sở dữ liệu hay được hỗ trợ bởi hệ quản trị cơ sở dữ liệu để hiện thực các chính sách và yêu cầu cho quy trình trên.

# ĐỀ 4: Xây dựng một ứng dụng website cho quy trình gia hạn hộ chiếu

## Mô tả chung quy trình gia hạn hộ chiếu

Gia hạn hộ chiếu dành cho các đối tượng đã được cấp hộ chiếu lần đầu.Thông tin để người sử dụng đăng ký gia hạn hộ chiếu bao gồm (Họ và tên, địa chỉ thường trú, phái, CMND, điện thoại, email, mã số hộ chiếu). Thông tin này sẽ được người đăng ký điền vào form online, nộp cho bộ phận xác thực **(XT)** và được lưu vào **Passport** database. Bộ phận này sau khi đối chiếu và kiểm chứng thông tin như CMND, hộ khẩu, mã số hộ chiếu …(giả sử các thông tin liên quan đến người đăng ký dùng để đối chiếu này được lưu trữ trong một database chung gọi là **Resident** database) sẽ gửi các yêu cầu đăng ký này cho bộ phận xét duyệt **(XD)**. Các yêu cầu đăng ký sau khi được phê duyệt sẽ được gửi đến bộ phận lưu trữ **(LT)** và thông báo kết quả cho người đăng ký. Song song đó bộ phận giám sát **(GS)** chịu trách nhiệm theo dõi và giám sát các hoạt động trên.

* [XT] bao gồm các bộ phận xác thực (kiểm chứng) được chia theo quận/huyện. Ví dụ [XTQ1] chịu trách nhiệm kiểm chứng các yêu cầu gia hạn hộ chiếu cho các đối tượng thuộc Quận 1. [XT] được quyền xem thông tin từ form đăng ký và thông tin liên quan đến người đăng ký (Resident Database) **ứng với mỗi quận. Nghĩa là [XTQ1] sẽ xem được dữ liệu ứng với quận 1.**
* [XD] có quyền xem tất cả các thông tin quy định gia hạn hộ chiếu và chỉ được xem thông tin trên form đăng ký. Không được xem thông tin trong Resident Database.
* [LT] chỉ được xem các thông tin được phê duyệt (đồng ý hay không đồng ý cấp hộ chiếu) và cập nhật lại thời hạn hộ chiếu được gia hạn, nhưng không xem được thông tin cá nhân và các dữ liệu liên quan khác.
* [GS] giám sát thông tin trạng thái của dữ liệu đăng ký qua từng bước (xác thực hay không, chờ xét duyệt, được duyệt hay không).

## Ghi chú

* Dữ liệu mẫu cho quy trình này SV tự thiết kế và nộp kèm theo kết quả xây dựng được.
* SV phải sử dụng các kỹ thuật bảo mật trong nội dung thực hành hoặc là các công nghệ khác liên quan đến bảo mật cơ sở dữ liệu hay được hỗ trợ bởi hệ quản trị cơ sở dữ liệu để hiện thực các chính sách và yêu cầu cho quy trình trên.

# ĐỀ 5: Xây dựng một ứng dụng cho quy trình quản lý nhân viên

## Mô tả chung chính sáchquản lý nhân viên

* Thông tin về nhân viên được lưu trữ gồm có: mã số, tên, ngày sinh, email, phòng ban đang làm việc, lương, mã số thuế. Mỗi một phòng ban có một trưởng phòng và quản lý mọi nhân viên trong phòng.
* Chính sách của công ty:
  + - * + Nhân viên của một phòng ban chỉ được xem mọi thông tin của các nhân viên cùng phòng ban với mình, ngoại trừ thông tin về lương. Lưu ý, chỉ được xem chứ không có quyền chỉnh sửa (insert, delete, update) thông tin, kể cả thông tin của mình.
        + Quản lý của phòng ban có quyền xem mọi thông tin của nhân viên trong phòng, kể cả thông tin về lương, tuy nhiên cũng không có quyền chỉnh sửa.
        + Đối với phòng HR (Human Resource):

Nhân viên phòng nhân sự có quyền xem, chỉnh sửa mọi thông tin của bất cứ nhân viên nào trong công ty, ngoại trừ nhân viên trong phòng của mình. (chính sách thứ nhất vẫn áp dụng cho nhân viên phòng nhân sự)

Trưởng phòng nhân sự có quyền xem và chỉnh sửa thông tin của mọi nhân viên, đồng thời có khả năng giám sát việc chỉnh sửa thông tin cá nhân của nhân viên trong phòng nhân sự.

* + - * + Đối với phòng kế toán: nhân viên phòng kế toán vẫn áp dụng chính sách thứ nhất. Tuy nhiên để tính lương cho nhân viên trong công ty thì nhân viên phòng kế toán có quyền xem mã số nhân viên, lương và mã số thuế của mọi nhân viên trong công ty.

## Ghi chú

* Dữ liệu mẫu cho quy trình này SV tự thiết kế và nộp kèm theo kết quả xây dựng được.
* SV phải sử dụng các kỹ thuật bảo mật trong nội dung thực hành hoặc là các công nghệ khác liên quan đến bảo mật cơ sở dữ liệu hay được hỗ trợ bởi hệ quản trị cơ sở dữ liệu để hiện thực các chính sách và yêu cầu cho quy trình trên.