Trường Đại học Khoa học Tự nhiên
Khoa Công nghệ thông tin

**NĂM HỌC 2022 – 2023, ĐỒ ÁN MÔN HỌC**

**CSC12001 - AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HTTT**

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

Sinh viên hãy xây dựng ứng dụng cho phép các người dùng có quyền quản trị thực hiện công việc sau:

- Xem danh sách người dùng trong hệ thống.
- Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu.
- Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user hoặc role.
- Cho phép thực hiện việc cấp quyền: cấp quyền cho user, cấp quyền cho role, cấp role cho user. 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). Quyền, select, update thì cho phép phân quyền tinh đến mức cột; quyền insert, delete thì không.
- Cho phép thu hồi quyền từ người dùng/ role.
- Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền.
- Cho phép chỉnh sửa quyền của user/ role.

## PHÂN HỆ 2:

Một công ty A có nhu cầu xây dựng một hệ thống S để quản lý thông tin nhân viên và việc tham gia đề án của nhân viên. Công ty dùng lược đồ CSDL như sau để lưu trữ một phần dữ liệu cần thiết:

**NHANVIEN (<u>MANV</u>, TENNV, PHAI, NGAYSINH, DIACHI, SODT, LUONG, PHUCAP, VAITRO, MANQL, PHG)**

Mỗi nhân viên có mã duy nhất (MANV), họ tên (TENNV), phái (PHAI), ngày sinh (NGAYSINH), địa chỉ (DIACHI), số điện thoại (SODT), lương (LUONG), phụ cấp (PHUCAP), người phụ trách trực tiếp, và phòng ban mà nhân viên trực thuộc (PHG). Thuộc tính VAITRO cho biết vai trò của một nhân viên và quyền truy cập cơ sở dữ liệu theo như mô tả về các chính sách bảo mật đối với từng vai trò bên dưới.

**PHONGBAN (<u>MAPB</u>, TENPB, TRPHG)**

Mỗi phòng ban có mã duy nhất, có tên phòng, có mã nhân viên làm trưởng phòng (TRPHG).

**DEAN (<u>MADA,</u> TENDA, NGAYBD, PHONG)**

Mỗi đề án có mã duy nhất (MADA), có tên duy nhất (TENDA), có ngày bắt đầu thực hiện đề án và do một phòng ban chủ trì việc phân công cho các nhân viên tham gia đề án đó.

**PHANCONG (<u>MANV, MADA</u>, THOIGIAN)**

Mỗi dòng của quan hệ phân công cho biết một nhân viên có mã là MANV được phân công tham gia đề án có mã là MADA với thời gian tham gia đề án là THOIGIAN.

Thuộc tính VAITRO trong quan hệ NHANVIEN:

- Cho biết nhiệm vụ của một nhân viên được tổ chức phân công, có thể nhận các giá trị sau: "Nhân viên", "QL trực tiếp", "Trưởng phòng", "Tài chính", "Nhân sự", "Trưởng đề án", "Ban giám đốc". Quyền tương ứng với từng vai trò được mô tả dưới dạng các chính sách được đánh mã CS#i bên dưới.
- Thuộc tính VAITRO phản ánh đúng vai trò:
    - "Trưởng phòng" nếu nhân viên là trưởng phòng (có mã nhân viên xuất hiện tại trường TRPHG của quan hệ PHONGBAN) hoặc
    - "QL trực tiếp" nếu nhân viên là quản lý trực tiếp (có mã nhân viên xuất hiện tại trường MANQL của quan hệ NHANVIEN).
    - Với những người dùng khác, vai trò của họ do người quản trị bảo mật trong hệ thống xác định giá trị tương ứng với nhiệm vụ đảm nhận trong công ty A, là một trong các giá trị mà thuộc tính VAITRO có thể nhận lấy, được liệt kê bên trên.

Sau đây là các giá trị cụ thể và quyền tương ứng của từng vai trò, được thể hiện dưới dạng các chính sách bảo mật CS#i:

**CS#1:** Những người dùng có thuộc tính VAITRO là **"Nhân viên"** cho biết đó là một nhân viên thông thường, không kiêm nhiệm công việc nào khác. Những người dùng có VAITRO là "Nhân viên" có quyền được mô tả như sau:

- Có quyền xem tất cả các thuộc tính trên quan hệ NHANVIEN và PHANCONG liên quan đến chính nhân viên đó.
- Có thể sửa trên các thuộc tính NGAYSINH, DIACHI, SODT liên quan đến chính nhân viên đó.

- Có thể xem dữ liệu của toàn bộ quan hệ PHONGBAN và DEAN.
- Hiện tại có 300 nhân viên trong toàn hệ thống S.

**CS#2:** Những người dùng có VAITRO là **"QL trực tiếp"** nếu họ phụ trách quản lý trực tiếp nhân viên khác. Nhân viên Q là quản lý trực tiếp nhân viên N, có quyền được mô tả như sau:

- Q có quyền như là một nhân viên thông thường (vai trò "Nhân viên"). Ngoài ra, với các dòng dữ liệu trong quan hệ NHANVIEN liên quan đến các nhân viên N mà Q quản lý trực tiếp thì Q được xem tất cả các thuộc tính, trừ thuộc tính LUONG và PHUCAP.
- Có thể xem các dòng trong quan hệ PHANCONG liên quan đến chính Q và các nhân viên N được quản lý trực tiếp bởi Q.
- Hệ thống S hiện tại có 20 người là quản lý trực tiếp.

**CS#3:** Những người dùng có VAITRO là "**Trưởng phòng**" cho biết đó là một nhân viên kiêm nhiệm thêm vai trò trưởng phòng. Một người dùng T có VAITRO là "Trưởng phòng" có quyền được mô tả như sau:

- T có quyền như là một nhân viên thông thường (vai trò "Nhân viên"). Ngoài ra, với các dòng trong quan hệ NHANVIEN liên quan đến các nhân viên thuộc phòng ban mà T làm trưởng phòng thì T có quyền xem tất cả các thuộc tính, trừ thuộc tính LUONG và PHUCAP.
- Có thể thêm, xóa, cập nhật trên quan hệ PHANCONG liên quan đến các nhân viên thuộc phòng ban mà T làm trưởng phòng.
- Hệ thống S hiện tại có 8 người là trưởng phòng.

**CS#4:** Những người dùng có VAITRO là "**Tài chính**" cho biết đó là một nhân viên phụ trách công tác tài chính tiền lương của công ty. Một người dùng có vai trò là "Tài chính" có quyền được mô tả như sau:

- Có quyền như là một nhân viên thông thường (vai trò "Nhân viên").
- Xem trên toàn bộ quan hệ NHANVIEN và PHANCONG, có thể sửa trên thuộc tính LUONG và PHUCAP (thừa hành ban giám đốc).
- Hệ thống S hiện tại có 5 người phụ trách công tác tài chính.

**CS#5:** Những người dùng có VAITRO là "**Nhân sự**" cho biết đó là nhân viên phụ trách công tác nhân sự trong công ty. Một người dùng có VAITRO là "Nhân sự" có quyền được mô tả như sau:

- Có quyền như là một nhân viên thông thường (vai trò "Nhân viên").
- Được quyền thêm, cập nhật trên quan hệ PHONGBAN.
- Thêm, cập nhật dữ liệu trong quan hệ NHANVIEN với giá trị các trường LUONG, PHUCAP là mang giá trị mặc định là NULL, không được xem LUONG, PHUCAP của người khác và không được cập nhật trên các trường LUONG, PHUCAP.
- Hệ thống S hiện tại có 5 người phụ trách công tác nhân sự.

**CS#6:** Những người dùng có VAITRO là "**Trưởng đề án**" cho biết đó là nhân viên là trưởng các đề án. Một người dùng là "Trưởng đề án" có quyền được mô tả như sau:

- Có quyền như là một nhân viên thông thường (vai trò "Nhân viên").
- Được quyền thêm, xóa, cập nhật trên quan hệ ĐEAN.
- Hệ thống S hiện tại có 3 người phụ trách công tác trưởng đề án.

Những người dùng có thuộc tính VAITRO là **"Ban giám đốc"** có quyền xem trên tất cả các bảng nhưng không có quyền thêm, xóa, sửa trên bất cứ bảng nào. Hiện tại có 5 người thuộc vai trò "Ban giám đốc". (Sinh viên không cần cài đặt chính sách này).

Cơ sở dữ liệu được cài đặt trên Hệ quản trị cơ sở dữ liệu **Oracle**. Hệ thống dùng chính sách đóng (người dùng *u* cần được cấp quyền *p* trên đối tượng dữ liệu *o* mới có thể thực hiện *p* trên *o*).

**Yêu cầu:**

1. Với vai trò là người quản trị bảo mật trong hệ thống S, em hãy mô tả thêm cho hệ thống chặt chẽ hơn và điều chỉnh lược đồ cơ sở dữ liệu nếu cần thiết và cấp quyền cho nhân sự trong toàn hệ thống theo các chính sách bảo mật CS#i.
2. Công ty A mong muốn hiện thực hóa hệ thống dưới hình thức một ứng dụng Winform theo mô hình Client-Server để phục vụ cho nhu cầu tra cứu và quản lý thông tin trong hệ thống. Để đảm bảo tính riêng tư về thông tin của nhân viên liên quan đến trường LUONG và PHUCAP, dữ liệu cần phải được bảo vệ thêm (ngoài cơ chế điều khiển truy cập) dùng cơ chế mã hóa dữ liệu. Sinh viên hãy đề xuất giải pháp mã hóa dữ liệu mà vẫn đảm bảo được

các chính sách bảo mật khác của hệ thống. Sinh viên có thể bổ sung hay điều chỉnh cấu trúc lưu trữ dữ liệu nếu cần. Sinh viên cần phân tích rõ trước khi cài đặt:

- User vai trò gì thực hiện mã hóa?
- Mã hóa dữ liệu ở mức nào (mức cơ sở dữ liệu, mức ứng dụng, …)? Vì sao chọn mức mã hóa đề nghị?
- Có cần thay đổi gì về cấu trúc lưu trữ dữ liệu hay không?
- Với phương pháp mã hóa dữ liệu đã đề xuất ở trên, sinh viên hãy trình bày các khía cạnh của cơ chế quản lý khóa đề nghị: thiết lập khóa, lưu trữ khóa, phân phối khóa, phục hồi khóa khi người dùng quên khóa, thay khóa đồng loạt sau một thời gian.

3. Người ta muốn thiết lập cho hệ thống S chức năng phát tán thông báo có mục tiêu đến những nhóm người dùng trong hệ thống tùy vào cấp bậc, lĩnh vực hoạt động và vị trí địa lý nơi nhân viên công tác. Cho biết người dùng (nhân viên) và dữ liệu được chia ra làm các cấp bậc sau: *giám đốc, trưởng phòng và nhân viên* và độ ưu tiên là: *giám đốc > trưởng phòng > nhân viên*. Hệ thống hoạt động ở 3 lĩnh vực: *mua bán, sản xuất, gia công*. Công ty có chi nhánh đặt tại ba nơi: *miền Bắc, miền Trung* và *miền Nam*. Cho biết cụ thể cách thiết lập hệ thống nhãn gồm 03 thành phần và những điều chỉnh mô hình dữ liệu (nếu có).
   a. Hãy gán nhãn cho 03 người dùng trong hệ thống:
      - 01 giám đốc có thể đọc được toàn bộ dữ liệu
      - 01 trưởng phòng phụ trách lĩnh vực sản xuất miền Nam
      - 01 giám đốc phụ trách bất kỳ lĩnh vực nào ở chi nhánh miền Bắc (có thể đọc được toàn bộ dữ liệu theo đúng cấp bậc và không phân biệt lĩnh vực).
   b. Hãy cho biết cách thức phát tán dòng thông báo t1 đến tất cả trưởng phòng phụ trách tất cả các lĩnh vực không phân biệt chi nhánh.
   c. Hãy cho biết cách thức phát tán dòng thông báo t2 đến trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung.
   d. Em hãy cho thêm một số kịch bản phát tán dữ liệu nữa trên mô hình OLS đã cài đặt.

4. Hãy cho biết cụ thể cách thức ghi vết (audit) các hành vi sau:
   a. Những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG.
   b. Những người đã đọc trên trường LUONG và PHUCAP của người khác.

c. Một người **không** thuộc vai trò "Tài chính" nhưng đã cập nhật thành công trên trường LUONG và PHUCAP.

d. Kiểm tra nhật ký hệ thống.

**MỘT SỐ QUY ĐỊNH:**

1. Các nhóm đều làm cả hai phân hệ, cùng ứng dụng.
2. Chấm đồ án vào ngày thi theo lịch thi chung của Trường.
3. Cuốn đồ án: trình bày lý thuyết ngắn gọn, dễ hiểu, ghi rõ tài liệu tham khảo, không dịch lại tài liệu, chủ yếu là phần tóm lược những gì tìm hiểu được, nhận xét, đánh giá, thuyết minh các kết quả đạt được. Nhóm trưởng làm bảng phân công công việc và đánh giá các thành viên trong nhóm (đóng chung trong cuốn đồ án). Ghi rõ nhóm đã cài đặt những chính sách bảo mật cụ thể nào, kịch bản gì. Nhóm cố gắng cài đặt tất cả các cơ chế bảo mật đã học.
4. Nộp file: ngoài bản in nộp vào ngày chấm đồ án, sinh viên phải nộp file trên Moodle, gồm file word báo cáo (file cuốn đồ án), source code. Tên file sẽ được quy định khi nộp bài.
5. Chia công việc sao cho tất cả các thành viên của nhóm đều phải thực hiện được yêu cầu của đồ án. Sinh viên có thể được yêu cầu phải thực hiện tại chỗ cài đặt một số chính sách bảo mật.
6. Bài giống nhau: tất cả đều 0 điểm.

**HẾT.**