**Trường Đại học Khoa học Tự nhiên**

**Khoa Công nghệ thông tin**

**MÔN AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ THỐNG THÔNG TIN**

**Bài tập vận dụng 1**

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 (MANV, 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 (MAPB, TENPB, TRPHG)**

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

**DEAN (MADA, 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 (MANV, MADA, 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 nhưng 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, 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*).

***Lưu ý:*** *Trong bài làm bên dưới, nếu sinh viên có dùng VPD để ép thỏa 1 chính sách bảo mật, chỉ cần nêu cách tạo vị từ của hàm chính sách và cách thức áp dụng chính sách. Nếu sinh viên có dùng view thì ghi định nghĩa view và cách thức phân quyền trên view. Sinh viên chỉ cần ghi cách làm và các câu lệnh chủ yếu để minh họa, không cần viết toàn bộ script.*

**Câu 1:** Với vai trò là người quản trị bảo mật trong hệ thống S, em hãy cho biết sử dụng những cơ chế bảo mật nào để hiện thực các chính sách bảo mật từ CS#1 đến CS#6.

Trình bày ngắn gọn cách thức tạo người dùng ban đầu.

**Câu 2:** Với vai trò là người quản trị bảo mật trong hệ thống S, em hãy trình bày cách thực hiện thực việc cấp quyền cho nhân sự trong toàn hệ thống theo từng chính sách bảo mật CS#i:

**Câu 3:** 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.

1. 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:
   1. 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 trình bày rõ mã hóa dữ liệu ở mức nào (mức cơ sở dữ liệu, mức ứng dụng, …)? Vì sao? Ai thực hiện mã hóa? Có cần thay đổi gì về cấu trúc lưu trữ dữ liệu hay không?
   2. 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.
2. Hãy phân tích ưu điểm và hạn chế của giải pháp đề xuất.

**Câu 4:** 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 tycó chi nhánh đặt tại ba nơi: *miền Bắc*, *miền Trung* và *miền Nam*.

1. Cho biết cụ thể cách thiết lập hệ thống nhãn gồm 03 thành phần và những điều chỉnh mô hình dữ liệu (nếu có).

* Level: GĐ > TP > NV
* Compartment: MB, SX, GC
* Group: MB, MT, MN

1. Hãy gán nhãn cho 03 người dùng trong hệ thống:

01 giám đốc có thể đọc được toàn bộ dữ liệu: GĐ

01 trưởng phòng phụ trách lĩnh vực sản xuất miền Nam: TP:SX:MN

01 giám đốc phụ trách cả 3 lĩnh vực ở chi nhánh miền Bắc (có thể đọc được toàn bộ dữ liệu theo đúng cấp bậc và không phân biệt lĩnh vực). GĐ: MB, SX, GC: MB

1. 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.: GĐ
2. Hãy cho biết cách thức phát tán dòng thông báo t2 đến trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung. TP:SX:MT

**Câu 4** Hãy cho biết cụ thể cách thức ghi vết (audit) các hành vi sau:

1. Những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG.
2. Những người đã đọc trên trường LUONG và PHUCAP của người khác.
3. Một người **không** thuộc vai trò “Tài chính” nhưng đã cập nhật thành công trên trường LUONG và PHUCAP.

**Bài tập vận dụng 2**

Sở y tế tỉnh/ thành phố X cần gom dữ liệu về kho dữ liệu D (cấp sở), gồm hồ sơ bệnh án (và một số dữ liệu liên quan) từ các cơ sở y tế trong tỉnh/ thành phố và quản lý chuyên môn về việc khám chữa bệnh của các cơ sở y tế thông qua một hệ thống thông tin quản lý S.

**HSBA (MÃHSBA, MÃBN, NGÀY, CHẨNĐOÁN, MÃBS, MÃKHOA, MÃCSYT, KẾTLUẬN):** mỗi hồ sơ bệnh án (HSBA) có một mã duy nhất (MÃHSBA), liên quan đến một bệnh nhân (MÃBN), được lập vào một ngày (NGÀY), có chẩn đoán (CHẨNĐOÁN) của bác sĩ điều trị (MÃBS), được tiếp nhận khám và điều trị tại khoa (MÃKHOA), của cơ sở y tế (có mã là MÃCSYT), với kết luận của bác sĩ (KẾTLUẬN).

**HSBA\_DV (MÃHSBA, MÃDV, NGÀY, MÃKTV, KẾTQUẢ):** ghi nhận lại các dịch vụ (thông qua MÃDV) đã sử dụng theo chỉ định của bác sĩ điều trị (ví dụ các loại xét nghiệm, chụp hình,…), người thực hiện dịch vụ (MÃKTV) và kết quả (KẾTQUẢ).

**BỆNHNHÂN (MÃBN, MÃCSYT, TÊNBN, CMND, NGÀYSINH, SỐNHÀ, TÊNĐƯỜNG, QUẬNHUYỆN, TỈNHTP, TIỀNSỬBỆNH, TIỀNSỬBỆNHGĐ, DỊỨNGTHUỐC):** mỗi bệnh nhân được cơ sở y tế có mã là MÃCSYT cấp mã duy nhất (MÃBN), có tên (TÊNBN), ngày sinh (NGÀYSINH), địa chỉ (SỐNHÀ, TÊNĐƯỜNG, QUẬNHUYỆN), và tiền sử bệnh của bệnh nhân (TIỀNSỬBỆNH) và gia đình (TIỀNSỬBỆNHGĐ), cũng như tình trạng dị ứng thuốc (nếu có, DỊỨNGTHUỐC).

**CSYT (MÃCSYT, TÊNCSYT, ĐCCSYT, SĐTCSYT):** ghi nhận thông tin về các cơ sở y tế thuộc tỉnh/ thành phố gồm mã, tên, địa chỉ, số điện thoại.

**NHÂNVIÊN (MÃNV, HỌTÊN, PHÁI, NGÀYSINH, CMND, QUÊQUÁN, SỐĐT, CSYT, VAITRÒ, CHUYÊNKHOA)**

Quan hệ NHÂNVIÊN chứa dữ liệu về các nhân viên trực thuộc cơ sở y tế hoặc thuộc sở y tế có vai trò trong hệ thống S. Mỗi nhân viên có mã (MÃNV) do đơn vị quản lý trực tiếp cấp, giả sử các mã này không trùng nhau trong phạm vi toàn tỉnh/ thành phố. Ngoài ra cũng cần ghi lại thông tin họ tên (HỌTÊN), phái (PHÁI), ngày sinh (NGÀYSINH), số chứng minh nhân dân (CMND), quê quán, số điện thoại, thuộc cơ sở y tế nào (CSYT). Thuộc tính VAITRÒ nhận một trong các giá trị sau: “Thanh tra”, “Cơ sở y tế”, “Y sĩ/ bác sĩ”, “Nghiên cứu”.

Với các nhân viên có vai trò “Y sĩ/ bác sĩ” hoặc “Nghiên cứu” thì cần lưu thêm thông tin về chuyên khoa (CHUYÊNKHOA) mà người đó được cấp bằng cấp chuyên môn.

Cơ sở dữ liệu được cài đặt trên **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*). DBA trong hệ thống S thực hiện việc cấp quyền cho nhân sự trong toàn hệ thống theo mô tả như sau:

**TC#1:** Ngoài DBA, tất cả người dùng trong hệ thống S gồm những nhân viên trong quan hệ NHÂNVIÊN và cả những bệnh nhân trong quan hệ BỆNHNHÂN. DBA tạo tài khoản cho tất cả những người dùng này. DBA không tự định nghĩa bảng (table) dùng để quản lý tài khoản người dùng mà sử dụng thông tin tài khoản do Hệ quản trị CSDL Oracle quản lý. Bằng cách nào DBA có thể kết nối một tên tài khoản với 1 dòng dữ liệu là người dùng tương ứng (trong quan hệ NHÂNVIÊN và BỆNHNHÂN) mà không phải truy cập dữ liệu từ nhiều hơn 1 bảng, đồng thời phải ép thỏa các chính sách bảo mật liên quan đến những người dùng này. DBA phụ trách thêm, cập nhật dữ liệu trong bảng CSYT và thêm dữ liệu trong NHÂNVIÊN, gồm những nhân viên thuộc các cơ sở y tế hoặc thuộc sở y tế có vai trò trong hệ thống S.

**TC#2:** Có 5 nhân viên thuộc sở y tế với vai trò “Thanh tra”. Các nhân viên giữ vai trò thanh tra có thể đọc dữ liệu trên tất cả các quan hệ được mô tả để kết xuất báo cáo định kỳ, mà không có quyền thêm, xóa, sửa trên bất cứ quan hệ nào.

**TC#3:** Mỗi cơ sở y tế được cấp duy nhất 01 tài khoản trên hệ thống S để thao tác trên kho dữ liệu D. Có 50 nhân viên thuộc 50 cơ sở y tế trong tỉnh/ thành phố được cử để sử dụng tài khoản được cấp. Các nhân viên thuộc cơ sở y tế có quyền thêm hoặc xóa dữ liệu phát sinh từ chính cơ sở y tế mà nhân viên này trực thuộc, trong tháng hiện tại từ ngày 5 đến 27 dương lịch hàng tháng, liên quan các nghiệp vụ:

a. Thêm, xóa dòng trên hồ sơ bệnh án (HSBA)

b. Thêm, xóa dòng dịch vụ (HSBA\_DV) liên quan 1 hồ sơ bệnh án.

**TC#4:** Có 500 nhân viên giữ vai trò “Y sĩ/ bác sĩ” trực tiếp khám chữa bệnh cho bệnh nhân ở các cơ sở y tế thuộc tỉnh/ thành phố. Y sĩ/ Bác sĩ có quyền xem hồ sơ bệnh án (HSBA) mà họ đã chữa trị và kết quả về các dịch vụ đã sử dụng (HSBA\_DV) và thông tin bệnh nhân (BỆNHNHÂN) khi nhập thông tin mã bệnh nhân hoặc số CMND.

**TC#5:** Có 50 nhân viên ở vai trò “Nghiên cứu” ở mỗi cơ sở y tế, chỉ có thể xem các hồ sơ bệnh án (bảng HSBA và HSBA\_DV) được điều trị tại cùng cơ sơt y tế (với nhân viên nghiên cứu đó), tại khoa giống chuyên khoa ghi trên bằng cấp của nhân viên nghiên cứu đó.

**TC#6:** Hệ thống hiện tại có khoảng 10000 bệnh nhân. Trên hệ thống S, trừ những người giữ vai trò thanh tra (và DBA), mỗi nhân viên hoặc bệnh nhân đăng nhập chỉ có thể xem thông tin của chính mình, (trên bảng NHÂN VIÊN nếu là nhân viên, trên bảng BỆNH NHÂN nếu là bệnh nhân), và có thể chỉnh sửa các trường (trừ trường mã) liên quan đến chính người đó.

**Câu 1:** Hãy trình bày cách thức hiện thực các chính sách bảo mật được mô tả ở dạng TC#i.

**Câu 2:** Sở Y tế tỉnh / thành phố X mong muốn hiện thực hóa hệ thống S 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.

1. Để đảm bảo tính riêng tư của thông tin bệnh nhân, dữ liệu liên quan đến bệnh nhân và hồ sơ bệnh án cần phải được bảo vệ bằng cơ chế mã hóa dữ liệu. Sinh viên hãy phân tích, lựa chọn đối tượng dữ liệu và thiết kế phương pháp mã hóa dữ liệu tương ứng cho hệ thống S nhưng vẫn đảm bảo được các chính sách bảo mật của hệ thống.
2. Với cơ chế bảo mật bằng phương pháp mã hóa dữ liệu đã đề xuất trên, sinh viên hãy thiết kế cơ chế quản lý khóa phù hợp với đối tượng sử dụng.

**Câu 3:** Dựa vào chuyên môn, kỹ thuật của đơn vị mà Sở y tế tỉnh/ thành phố X chia các cơ sở y tế trực thuộc thành 3 tuyến:

* *“Điều trị ngoại trú”*: các cơ sở khám chữa bệnh ban đầu, điều trị ngoại trú.
* *“Điều trị nội trú”*: các bệnh viện với các kỹ thuật chuyên khoa cơ bản và nâng cao.
* *“Điều trị chuyên sâu”*: các bệnh viện đa khoa và chuyên khoa thực hiện được các kỹ thuật chuyên sâu.

Ngoài ra, tùy vào vị trí địa lý của cơ sở y tế mà Sở y tế tỉnh/ thành phố X chia ra làm 3 vùng: *trung tâm, cận trung tâm, ngoại thành*. Có sự phân chia vai trò người dùng theo 03 cấp bậc: **Giám đốc sở**, **Giám đốc cơ sở y tế** và **Y/ Bác sĩ**. Sở cần gửi những dòng trong quan hệ THÔNGBÁO, gồm các trường NỘIDUNG, NGÀYGIỜ và ĐỊAĐIỂM về những cuộc họp khẩn đến các vai trò liên quan ở các cơ sở y tế. Dùng OLS (Oracle Label Security), hãy:

1. **(**Cho biết cụ thể cách thiết lập hệ thống nhãn gồm 03 thành phần và những điều chỉnh mô hình dữ liệu (nếu có).:

* Level: GĐS > GĐCSYT > Y/BS
* Compartment: NgT, NT, CS
* Group: TT, CTT, NgT

1. Gán nhãn cho 03 người dùng trong hệ thống: 01 giám đốc sở (có thể đọc được toàn bộ dữ liệu), 01 giám đốc cơ sở điều trị ngoại trú vùng trung tâm, 01 y/ bác sĩ vùng ven (có thể đọc được toàn bộ dữ liệu theo đúng cấp bậc và không phân biệt tuyến).

* GĐS
* GĐCSYT: NgT: TT
* Y/BS: NgT, NT, CS: NgT

1. Hãy cho biết cách thức phát tán dòng thông báo t1 đến tất cả giám đốc của tất cả các cơ sở y tế trực thuộc sở.

* GĐCSYT

1. Hãy cho biết cách thức phát tán dòng thông báo t2 đến giám đốc các đơn vị điều trị chuyên sâu ở vùng trung tâm.

* GĐCSYT: CS: TT

**Câu 4** Hãy cho biết cách thức ghi vết 4 thao tác bất hợp pháp gồm thêm, xóa, sửa, tìm kiếm dựa trên những hành vi vi phạm các chính sách bảo mật mô tả ở đề bài liên quan đến quan hệ HSBA.