**2001 - An toàn bảo mật dữ liệu trong HTTT**

**HK2 2024-2025**

**Chương trình chính quy chuẩn- Lớp 22HTTT1**

GVLT:

Cô Phạm Thị Bạch Huệ

Thầy Lương Vĩ Minh

Trợ giảng:

Cô Tiết Gia Hồng

TH:

Thầy Lương Vĩ Minh

| **Lần đánh giá** | **Nội dung** | **Hình thức** | **Tỉ lệ** |
| --- | --- | --- | --- |
| **Thi viết lý thuyết** | Phân tích các yêu cầu về bảo mật của một HTTT | Viết cá nhân, 90 phút, được mang theo 1 tờ A4 (2 mặt) | 40 % |
| **LT giữa kỳ** | SQL Injection. |  | 10% |
| **Đồ án** | Phân tích và đề ra giải pháp cho 1 HTTT, cài đặt ép thỏa các chính sách bảo mật Ra đề đồ án ngay từ đầu HK. | 4 SV/ đồ án Phân hệ 1:  Phân hệ 2: | 30% |
| **Thực hành** | Bài tập phần thực hành theo yêu cầu của GV HDTH ĐKTC, Mã hóa | Theo nội dung thực hành | 20% |

Hệ thống môn học

1. CSDL
2. HQT CSDL
3. CSDL nâng cao
4. ATBM HTTT
5. PTTK HTTT

* Lab Exercise : 20%

→ làm bài tập các nội dung lý thuyết (XTND, ĐKTC), mã hóa.

* Project Oral test : 30%

→ làm nhóm 4 thành viên.

xác thực người dùng, ĐKTC, Audit, hiểu cách quản lý system objects (Data Dictionary) của HQT CSDL.

* Mid-term Exam : 10%

→ SQL Injection: đọc bài trước (làm bài kiểm tra trên lớp).

* Final Exam : 40%

→ cá nhân, cho một đề dạng phân tích ứng dụng thực tế

Thi cuối kỳ: không kiểm tra các nội dung: SQL injection, mã hóa.

Nội dung thi cuối kỳ: xác thực người dùng, ĐKTC, Audit.

SV cài Oracle càng sớm càng tốt.

Sử dụng HQT CSDL mới bằng cách “dời” kiến thức đã biết từ SQL Server sang Oracle.

1. Đọc và xác định các loại người dùng và cho biết em có thể đóng vai trò là loại người dùng nào.
2. Thực hiện bài tập 1.

Bài tập nhóm

Chia sẻ quyền đọc trên file bài làm cho [ptbhue@fit.hcmus.edu.vn](mailto:ptbhue@fit.hcmus.edu.vn)

| Nhóm | Đường dẫn | Thành viên |
| --- | --- | --- |
| 1 | [Nhóm 1](https://docs.google.com/document/d/1krYQVaTDsWrfsvGYMW4JDiBjJ-bKKe_jsbDNrTjNXXA/edit?tab=t.0) | 22127157 - Nguyễn Quang Huy  22127218 - Văn Bá Đức Kiên  22127452 - Lê Ngọc Vĩ  22127411 - Lê Thị Thanh Thùy |
| 2 | [Nhóm 2](https://docs.google.com/document/d/1kRfNtk7-W2gqXPKfOZ471d5UkLHD1ariFjuG6SDkB9o/edit?usp=sharing) | 22127327 - Trần Quốc Phong  22127342 - Bùi Minh Quân  22127343 - Huỳnh Minh Quân  22127426 - Đinh Duy Triết |
| 3 | [Nhóm 3](https://docs.google.com/document/d/15qNS-o1U1gF4zEKBVxjcBU6ILXHAnZXjlVMzccM6PKg/edit?usp=sharing) | 22127192 - Trần Gia Khiêm  22127367 - Nguyễn Hữu Trường Sơn  22127413 - Phạm Hoàng Tiên  22127355 - Nguyễn Trần Đại Quốc  22127371 - Ngô Tấn Tài |
| 4 | [Nhóm 4](https://docs.google.com/document/d/13ox9i1HpquuR0g6qictU3xXdK64bRtOO1BJFseR5epw/edit?usp=sharing) | 22127103 - Lê Thị Hồng Hạnh  22127162 - Phan Thành Quang Huy  22127158 - Nhâm Đức Huy  22127433 - Nguyễn Ngọc Anh Tú |
| 5 | [Nhóm 5](https://docs.google.com/document/d/11-Hu4SZMxoNLHJI1U_0viEokOiqnK91x-c8cYMLrfS8/edit?tab=t.0#heading=h.scrzb166b65c) | 22127470 - Lê Hoàng Yến  22127197 - Nguyễn Đăng Khoa  22127247 - Nguyễn Thế Thanh Long  22127356 - Trần Nguyễn Lộc Quý |
| 6 | [Nhóm 6](https://docs.google.com/document/d/11Zv3fsho8k7FfYm8mCbaLbzWdC1dpeSCuSY5DkaZXM0/edit?usp=sharing) | 22127069 - Nguyễn Đặng Hoàng Dinh  22127139 - Hoàng Duy Hưng  22127334 - Lý Anh Quân  22127453 - Trần Tường Vĩ |
| 7 | Nhóm 7 |  |

**Xác thực người dùng (user authentication) - Không phận sự miễn vào**

**Yêu cầu nộp bài: Em hãy trình bày hiểu biết của em về cơ chế xác thực người dùng.**

**Làm theo nhóm, tìm hiểu và viết bài theo bố cục được tổ chức rõ ràng, đầy đủ nội dung.**

**Nộp trên Moodle, deadline sáng T3, 8:00 am.**

**Làm theo nhóm áp dụng hôm nay.**

**Gợi ý:**

Định nghĩa.

Quá trình: đăng ký (hệ thống đóng/ mở), xác thực/ so khớp.

Vai trò.

Các phương pháp: username + pw, thẻ, đặc trưng sinh trắc (vân tay, mống mắt, face id, …, ),

Chi phí,

Ưu khuyết điểm

Độ an toàn: các loại tấn công (replay attack?), …

Phù hợp hoàn cảnh nào

Khuyến cáo

Với vai trò là DBA

* Không chia sẻ dữ liệu chi tiết. Chọn giải pháp dùng view chia sẻ dữ liệu thống kê (sum. Count, ..)
* Các trường chứa thông tin quan trọng hãy lược bỏ khỏi đối tượng dữ liệu chia sẻ dùng view.
* Dùng hàm DECODE (hoặc IIF) để vẫn cho truy cập (các) trường nhạy cảm nhưng cần thỏa điều kiện.
* Thông qua view, cập nhật 1 trường của base table(s).
  + Chỉ có quyền trên view.
  + Cấp thêm quyền để có thể thực hiện cập nhật trên base table(s).
  + Thao tác (Select, Insert, Update, Delete) trên dòng dữ liệu liên quan đến chính mình.

1. **Trong một hệ thống nói chung, có phải lúc nào chúng ta cũng cần dùng cơ chế xác thực người dùng?**
2. **Cơ sở để em chọn dùng 1 phương pháp xác thực người dùng nào đó?**
3. **Các nguy cơ tấn công nhằm vào cơ chế xác thực người dùng?**
4. **Em làm gì để tăng tính an toàn cho 1 phương pháp xác thực?**

**Mức độ bảo mật**

**Chi phí**

**Khả năng mở rộng**

**Trải nghiệm người dùng**

**Cơ chế bảo mật (Security Mechanism) HQT CSDL**

1. **Xác thực người dùng - User Authentication:**
2. **Điều khiển truy cập- Access Control - User Authorization:**
3. **Mã hóa**
4. **Audit**

**Điều khiển truy cập- Access Control - User Authorization:**

1. **Dùng view:**

* Dùng view để che giấu thông tin chi tiết mà chỉ chia sẻ thông tin tổng quát cần thiết
* Dùng view để giới hạn thuộc tính cần chia sẻ
* Dùng DECODE để tránh TH người dùng truy cập 1 số giá trị của người khác
* Dùng view sử dụng hàm SYS\_CONTEXT() để ép thỏa các chính sách bảo mật dạng “cập nhật thông tin của chính mình”
* View là một đối tượng của CSDL. Ta có thể tạo view khi cần.
* Các cơ chế AC đều có thể dùng view nếu cần thiết.

1. **VPD**
2. **OLS**

**Bài tập nhóm**

1. **Phát biểu các chính sách bảo mật (security policy) liên quan từng nhóm người dùng/ role.**

**Sinh viên được:**

* **xem trên bảng COURSE**
* **Xem trên bảng SINHVIEN liên quan dòng của chính mình.**
* **Xem trên GRADE\_REPORT liên quan dòng của chính mình.**

**Giảng viên được:**

1. **Biết rằng có những loại người dùng sau và số thể hiện người dùng tương ứng.**

**● Sinh viên - Student: 3**

**● Giảng viên- Instructor: 3**

**● Chuyên viên phòng đào tạo: 3**

**● Nhân viên phòng khảo thí: 3**

**● Chuyên viên phòng công tác sinh viên: 3**

**Hãy ép thỏa các chính sách bảo mật mà em đã phát biểu ở 1 bằng 2 cơ chế AC khác nhau:**

1. **DAC.**
2. **RBAC.**
3. **VPD**

**1 nhóm cung cấp bài làm, cô sửa làm bài làm tham khảo.**

**NHANVIEN (MANV, TENNV, PHAI, NGAYSINH, DIACHI, SODT, LUONG, un, PHUCAP, VAITRO, MANQL, PHG)**

**VAITRO:**

1. **“Nhân viên”: 100**

* Có quyền xem tất cả các thuộc tính trên quan hệ NHANVIEN liên quan đến chính nhân viên đó.

- Có thể sửa trên các thuộc tính NGAYSINH, DIACHI, SODT liên quan đến chính nhân viên đó.

1. **“QL trực tiếp”: 20**

* 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.

1. **“Trưởng phòng”: 5**

* 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 làm trưởng phòng thì T có quyền xem tất cả các thuộc tính, trừ thuộc tính LUONG và PHUCAP.

1. **“Tài chính”: 5**

* Có quyền như là một nhân viên thông thường (vai trò “Nhân viên”).
* Xem trên toàn bộ quan hệ NHANVIEN, có thể sửa trên thuộc tính LUONG và PHUCAP (thừa hành ban giám đốc).

1. **“Nhân sự”: 5**

* Có quyền như là một nhân viên thông thường (vai trò “Nhân viên”).
* sýThêm, 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.

1. **“Trưởng đề án”:1**

* Có quyền như là một nhân viên thông thường (vai trò “Nhân viên”).

1. **“Ban giám đốc”: 3**

* Có quyền xem tất cả các thuộc tính trên quan hệ NHANVIEN.

**Em ép thỏa các chính sách bảo mật 1 đến 7 dùng:**

1. **DAC?**

**Tạo view:**

**View lọc dữ liệu chính mình: xem, sửa**

**View dành QL Trực tiếp**

**View dành Trưởng phòng**

**View dành cho Nhân sự**

1. **RBAC?**
2. **VPD?**

**Các vị từ ứng với từng loại người dùng.**

**Bài tập về nhà:**

1. **Với BT 1, bổ sung thêm yêu cầu “VPD”**
2. **Thực hiện nhóm BT2**

**Xem trước bài giảng OLS:**

* **Level**
* **Compartment**
* **Group**
* **Label**
* **Xem thuật toán đọc**

**Xem trước bài Audit (cô sẽ gửi bài giảng)**

**Bài tập vận dụng**

Cho lược đồ CSDL sau:

1. NHANVIEN (MANV, HONV, TENLOT, TENNV, PHAI, LUONG, DIACHI, NGAYSINH, MANQL, PHG)

2. PHONGBAN (MAPB, TENPB, TRPHG, NGAYBĐ)

3. DIADIEM\_PHG (MAPB, DIADIEM)

4. DEAN (MADA, TENDA, NGAYBD, PHONG, DIADIEM\_DA)

5. PHANCONG (MANV, MADA, THOIGIAN)

6. THANNHAN(MANV, TENTN, PHAI, NGSINH,QUANHE)

| STT | Chính sách bảo mật | DAC/RBAC (dùng view nếu cần) | VPD |
| --- | --- | --- | --- |
| 1 | Nhân viên chỉ được xem dữ liệu liên quan đến chính nhân viên đó, dba được truy cập tất cả. | CREATE OR REPLACE VIEW NV\_Xem\_NHANVIEN  AS  SELECT \* FROM NHANVIEN  WHERE MANV = SYS\_CONTEXT ('userenv', 'session\_user')  ~~WITH CHECK OPTION;~~ | Create function Xem\_NHANVIEN (p\_schema varchar2, p\_obj varchar2)  Return varchar2  As  user VARCHAR2(100);  Begin  if ( SYS\_CONTEXT(‘userenv’, ‘ISDBA’) ) then  return ‘ ’;  else user := SYS\_CONTEXT(‘userenv’, ‘SESSION\_USER’); return ‘MANV = ‘ || user;  end if; End;   * Áp dụng chính sách: |
|  | Nhân viên có thể xem mọi dòng dữ liệu trong bảng NHANVIEN, nhưng chỉ có chính họ mới có thể xem thông tin cột LUONG của họ. | CREATE OR REPLACE VIEW NV\_Xem\_NHANVIEN  AS  SELECT MANV, HONV, TENLOT, TENNV  DECODE (MANV, USER, LUONG, NULL) LUONGNV  FROM NHANVIEN;  Nếu cấp quyền trực tiếp cho từng nhân viên:  Grant select on NV\_Xem\_NHANVIEN to nv1  Hoặc nếu dùng role thì cấp quyền select trên NV\_Xem\_NHANVIEN cho role r\_NHANVIEN | Create function NV\_Xem\_NHANVIEN(p\_schema varchar2,  p\_obj varchar2)  Return varchar2  As  user VARCHAR2(100);  Begin  user := SYS\_CONTEXT(‘userenv’, ‘SESSION\_USER’); return ‘MANV = ‘ || user; end if;  End;  Áp dụng chính sách:  sec\_relevant\_cols =>’LUONG’, sec\_relevant\_cols\_opt => dbms\_rls.ALL\_ROWS); |
|  | Trưởng phòng được xem thông tin của chính họ và (các) nhân viên thuộc phòng ban mà họ làm trưởng.  Người quản lý trực tiếp có thể xem thông tin của họ và (các) nhân viên thuộc quyền quản lý trực tiếp của mình.  Trong cả hai trường hợp trên, dữ liệu kết xuất không kể lương. | CREATE CONTEXT people\_ctx USING sec\_mgr.people\_ctx\_mgr;  CREATE OR REPLACE PACKAGE people\_ctx\_mgr AS PROCEDURE set\_deptno; PROCEDURE clear\_deptno;  END;  CREATE OR REPLACE PACKAGE BODY people\_ctx\_mgr AS  PROCEDURE set\_deptno  AS  l\_deptno NUMBER; BEGIN  SELECT deptno INTO l\_deptno FROM lookup\_dept WHERE username = SYS\_CONTEXT ('MANV', 'session\_user’);  DBMS\_SESSION.set\_context (namespace => 'people\_ctx’,  ATTRIBUTE => 'deptno’,  VALUE => l\_deptno);  END set\_deptno;  PROCEDURE clear\_deptno  AS BEGIN  DBMS\_SESSION.CLEAR\_CONTEXT(namespace =>'people\_ctx', ATTRIBUTE => 'deptno');  END clear\_deptno;  END people\_ctx\_mgr;  CREATE OR REPLACE TRIGGER set\_user\_deptno  AFTER LOGON ON DATABASE  BEGIN  Sec\_mgr.people\_ctx\_mgr.set\_deptno;  EXCEPTION  WHEN NO\_DATA\_FOUND  THEN  -- If user is not in table,  -- a no\_data\_found is raised  -- If exception is not handled, then users not in table  -- will be unable to log on  NULL;  CREATE OR REPLACE VIEW quanly\_nv AS  SELECT NV.MANV, NV.HONV, NV.PHG  FROM NHANVIEN NV  WHERE  NV.PHG = SYS\_CONTEXT('people\_ctx', 'deptno')  OR  NV.MANQL = SYS\_CONTEXT('people\_ctx', 'MANV');  —---------------  CREATE OR REPLACE VIEW NV\_Xem\_NHANVIEN  AS  SELECT MANV, HONV, TENLOT, TENNV FROM NHANVIEN  WHERE PHG = SYS\_CONTEXT ('usernv', 'session\_user')  dùng role thì cấp quyền select trên TRPHG\_Xem\_NHANVIEN cho role r\_TRPHG: Grant SELECT on TRPHG\_Xem\_NHANVIEN to r\_TRPHG  —----  // Bổ sung: View cho ra kết quả mong muốn là gì?  CREATE OR REPLACE VIEW TPQL\_NV  AS  SELECT NV.MANV, NV.HONV, NV.TENLOT, NV.TENNV, NV.PHAI, NV.DIACHI, NV.NGAYSINH, NV.MANQL, NV.PHG, NV.USERNAME  FROM NHANVIEN TP\_QL  LEFT JOIN PHONGBAN PB ON TP\_QL.MANV = PB.TRPHG  JOIN NHANVIEN NV ON (PB.MAPB = NV.PHG OR NV.MANQL = TP\_QL.MANV OR TP\_QL.MANV = NV.MANV)  WHERE TP\_QL.USERNAME = SYS\_CONTEXT('userenv', 'session\_user')  —--------------------  Các khác: Tạo 2 view dành cho 2 đối tượng: trưởng phòng và người quản lý trực tiếp  CREATE OR REPLACE VIEW TP\_NV  AS  SELECT NV.MANV, NV.HONV, NV.TENLOT, NV.TENNV, NV.PHAI, NV.DIACHI, NV.NGAYSINH, NV.MANQL, NV.PHG, NV.USERNAME  FROM NHANVIEN TP\_NV  WHERE TP\_NV.USERNAME = SYS\_CONTEXT('userenv', 'session\_user')  CREATE OR REPLACE VIEW QLTT\_NV  AS  SELECT MANV, HONV, TENLOT, TENNV, PHAI, DIACHI, NGAYSINH, MANQL, PHG, USERNAME  FROM NHANVIEN  WHERE MANQL = SYS\_CONTEXT(‘userenv’, ‘session\_user’) OR MANV = SYS\_CONTEXT(‘userenv’, ‘session\_user’) | CREATE OR REPLACE FUNCTION(  p\_schema VARCHAR2,  p\_obj VARCHAR2  )  RETURN VARCHAR2  AS  user VARCHAR2  phg VARCHAR2  BEGIN  user = SYS\_CONTEXT('USERENV', 'SESSION\_USER')  phg = SELECT p.MAPB INTO phg FROM PHONGBAN p WHERE TRPHG = user  RETURN 'MANV = ' || user || ' OR PHG = ' || phg || ' OR MANQL = ' || user  END  Áp dụng chính sách:  sec\_relevant\_cols =>’LUONG’,  sec\_relevant\_cols\_opt => dbms\_rls.ALL\_ROWS); |
|  | Hãy tạo ra chính sách bảo mật không cho truy xuất (select) đến dòng nào của một bảng dữ liệu (dùng cách thông thường và dùng VPD). | Không tường minh cấp quyền đọc cho tất cả user thì bảng đó không ai có quyền đọc. | “1 = 2” |
|  | Hãy tạo ra chính sách bảo mật biến 1 bảng dữ liệu thành bảng chỉ đọc (Read-Only) (dùng cách thông thường và dùng VPD). | Cấp quyền đọc cho các user có quyền trong hệ thống.  GRANT [with grant option]  REVOKE  DENY | “1=0” áp dụng với Insert, Update, Delete |

**VPD:**

**NV: LUONG > 2000**

1. **Áp dụng vị từ p trên NV thì mọi user được quyền select trên NV theo vị từ p.**
2. **Áp dụng vị từ p trên NV thì user được quyền select trên NV theo vị từ p khi các user được cấp quyền select tường minh trên NV.**
3. **Trong một hệ thống chúng ta có thể sử dụng nhiều cơ chế bảo mật khác nhau không? Giải thích?**
4. **Trong một hệ thống chúng ta có thể sử dụng nhiều cơ chế ĐKTC khác nhau không? Giải thích?**

**(DAC, RBAC, VPD, OLS)**

**TL1: Có thể áp dụng DAC và RBAC cùng lúc.**

**TL2: Có thể áp dụng nhiều cơ chế bảo mật khác nhau trong một hệ thống vì 1 hệ thống có thể có nhiều chính sách bảo mật, tùy vào chính sách bảo mật sẽ chọn cơ chế phù hợp nên có thể có nhiều cơ chế khác nhau.**

**TL3:**

* **Có thể dùng Authentication để xác nhận đăng nhập**
* **Dùng RBAC và DAC để điều khiển truy xuất.**
* **Dùng Data Encryption để mã hóa dữ liệu (vd: truyền tải dữ liệu giữa server và client)**

**→ Nên hoàn toàn có thể sử dụng nhiều cơ chế bảo mật khác nhau cùng phối hợp cho một hệ thống.**

**Audit.**

**Tìm keyword này:**

**The Oracle Label Security Algorithm for Read Access**

**The Oracle Label Security Algorithm for Write Access**

**Làm bài tập lý thuyết, Bài tập 2 thư mục Homework, làm theo nhóm, nộp trên Moodle, nộp ngày 11/03/2025.**

**Ghi chú: Bài tập 2 gồm 2 bài tập vận dụng.**

**Bài tập 2 - Bài tập vận dụng 1 - Câu 4**

**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).
2. 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 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).

1. Hãy cho biết cách thức phát tán dòng thông báo t1 đến các trưởng phòng phụ trách đồng thời 3 lĩnh vực ở bất cứ chi nhánh nào

Các ví dụ về nhãn của người dùng:

TP: MB, SX, GC: B

TP: MB, SX, GC: T

TP: MB, SX, GC: N

TP: MB, SX, GC: B, T, N

1. Hãy cho biết cách thức phát tán dòng thông báo t1’ đến các trưởng phòng phụ trách bất cứ lĩnh vực nào, bất cứ chi nhánh nào.

Vài ví dụ về nhãn của người dùng:

TP: SX: B

TP: MB: B

TP: GC: B

1. 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: T

**Bài làm**

1. Level: GD > TP > NV

Compartment: MB, SX, GC

Group: B, T, N

1. 01 giám đốc có thể đọc được toàn bộ dữ liệu -> GD:MB,SX,GC:B,T,N

01 trưởng phòng phụ trách lĩnh vực sản xuất miền Nam -> TP:SX:N

01 giám đốc phụ trách cả 3 lĩnh vực ở chi nhánh miền Bắc -> GD:MB,SX,GC:B

1. TP:MB,SX,GC:B,T,N

TP: MB, SX, GC

1. TP
2. TP:SX:T

**Bài tập 2 - Bài tập vận dụng 1 - Câu 3**

**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).
2. 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).
3. 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.
4. 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.

**Bài làm**

1. Level: GDS > GDCS > Y/BS

Compartment: NgT, NT, CS

Group: TT, CTT, NT

1. 1 giám đốc sở có thể đọc toàn bộ dữ liệu: GĐS:NgT,NT,CS:TT,CTT,NT

1 giám đốc cơ sở điều trị ngoại trú vùng trung tâm: GDCS:NT:TT

1 y/bác sĩ vùng ven:Y/BS:NgT, NT, CS:NT

1. GDCS
2. GDCS:CS:TT

Audit

1. Lý do?
2. Cách kích hoạt.
3. Audit thông thường (standard audit)
4. FGA - Fine-grained Audit.
5. Cách đọc dữ liệu audit được.

**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.

Ghi vết các thao tác cập nhật các trường liên quan đến điểm (ĐIEMTH, ĐIEMQT, ĐIEMCK, ĐIEMTK) trên quan hệ ĐANGKY.

DBMS\_FGA.add\_policy

object\_schema => 'SV’,

object\_name => ‘ĐANGKY’,

policy\_name => 'capnhatdiem',

audit\_column => 'ĐIEMTH, ĐIEMQT, ĐIEMCK, ĐIEMTK’,

statement\_types => ‘update’);

Bài làm

1. Standard: AUDIT UPDATE ON PHANCONG BY ACCESS;

FGA: DBMS\_FGA.add\_policy(

object\_schema => ‘?’,

object\_name => ‘PHANCONG’,

policy\_name => ‘capnhatthoigian’,

‘Audit\_column => ‘THOIGIAN’,

statement\_types => ‘update’);

1. Standard:

FGA: DBMS\_FGA.add\_policy(

object\_schema => ‘NV’

object\_name => ‘NHANVIEN’,

policy\_name => ‘docluongvaphucap’,

Audit\_condition => ‘MANV != USER’

audit\_column => ‘LUONG, PHUCAP’,

statement\_types => ‘select’);

1. Standard: AUDIT SELECT ON

FGA: DBMS\_FGA.add\_policy(

object\_schema => ‘NV’

object\_name => ‘NHANVIEN’

policy\_name => ‘khongTaiChinhCapNhat’

audit\_condition => ‘VAITRO != “Tai chinh”’

audit\_column => ‘LUONG, PHUCAP’,

statement\_types => ‘update’);