TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

**KHOA CÔNG NGHỆ THÔNG TIN**

# BÁO CÁO ĐỒ ÁN

# NHÓM 11

MÔN HỌC

**AN TOÀN VÀ BẢO MẬT TRONG HỆ THỐNG THÔNG TIN**

CHƯƠNG TRÌNH CHÍNH QUY

**GIÁO VIÊN LÝ THUYẾT**

TS. Phạm Thị Bạch Huệ

**GIÁO VIÊN HƯỚNG DẪN THỰC HÀNH**

ThS. Lương Vĩ Minh

**THÔNG TIN NHÓM**


| | |
|---|---|
| Lê Minh Quân | 20120356 |
| Lê Phước Toàn | 20120386 |
| Lâm Nhựt Trường | 20120611 |
| Nguyễn Thị Bích Trâm | 20120389 |

# MỤC LỤC

# BẢNG PHÂN CHIA CÔNG VIỆC

**PHÂN HỆ 1:**

| MSSV | Họ Tên | Công việc |
|---|---|---|
| **20120356** | Lê Minh Quân | • 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 cấpquyền có thể cấp quyền đó cho user/ rolekhác hay không (có chỉ định WITHGRANT OPTION hay không).Quyền,select, update thì cho phép phân quyền tinh đến mức cột; quyền insert, delete thì không.<br>• Quay video demo phần của bản thân. |
| **20120386** | Lê Phước Toàn | • Login – Đăng nhập hệ thống.<br>• Xem danh sách người dùng hệ thống.<br>• Quay video demo phần của bản thân. |
| **20120611** | Lâm Nhựt Trường | • Cho phép tạo mới, xóa, sửa user/role.<br>• Báo cáo.<br>• Quay video demo phần của bản thân. |
| **20120389** | Nguyễn Thị Bích Trâm | • Cho phép kiểm tra quyền của chủ thể vừa được cấp quyền.<br>• Cho phép thu hồi quyền từ user/role.<br>• Cho phép chỉnh sửa quyền của user/role.<br>• Quay video demo phần của bản thân. |

**PHÂN HỆ 2:**

| MSSV | Họ Tên | Công việc |
|---|---|---|
| **20120356** | Lê Minh Quân | • Cài đặt các chính sách bảo mật CS#4, CS#5 và giao diện người dùng tương ứng.<br>• Cài đặt chính sách mã hóa.<br>• Lập báo cáo |
| **20120386** | Lê Phước Toàn | • Tạo khung giao diện cho toàn bộ ứng dụng và xử lý Login.<br>• Cài đặt các chính sách bảo mật CS#1 và giao diện người dùng tương ứng.<br>• Hỗ trợ cài đặt chính sách mã hóa.<br>• Lập báo cáo |
| **20120611** | Lâm Nhựt Trường | • Cài đặt các chính sách bảo mật CS#2 , CS#3 và giao diện người dùng tương ứng.<br>• Cài đặt Auditing cho hệ thống.<br>• Lập báo cáo |
| **20120389** | Nguyễn Thị Bích Trâm | • Cài đặt chính sách bảo mật CS#6 và giao diện người dùng tương ứng.<br>• Cài đặt OLS và mô tả các ngữ cảnh có thể xảy ra.<br>• Lập báo cáo. |

# NỘI DUNG

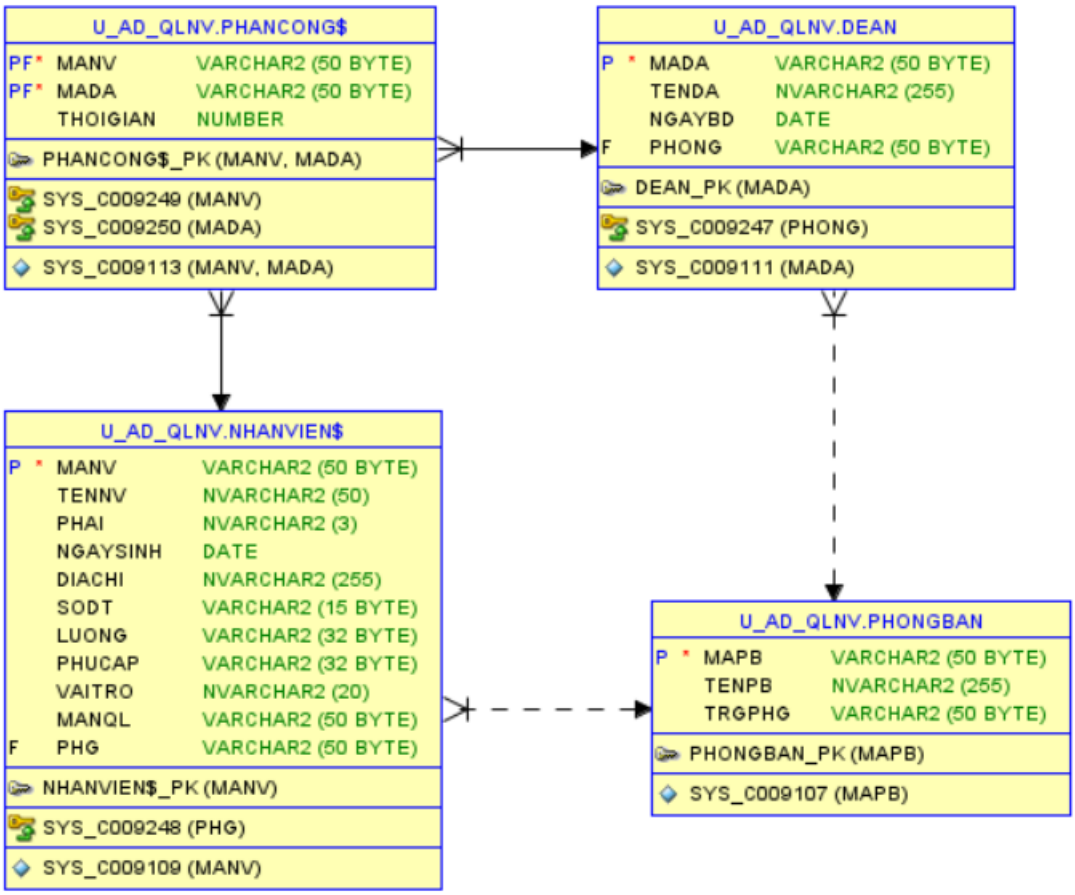
## 1. PHÂN HỆ 1

- Nhóm đã hoàn thành tất cả các chức năng của Phân hệ 1.

- 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.

# 2. PHÂN HỆ 2

## 2.1. Mô hình CSDL




## 2.2. Đặc tả dữ liệu

- Để phục vụ cho việc cài đặt các chính sách bảo mật của phân hệ 2, cho nên bảng CSDL thay đổi 2 bảng sau đây:

+ NHANVIEN được đổi thành NHANVIEN$ cột LUONG và PHUCAP được thay đổi để phù hợp cho việc mã hóa.

+ PHANCONG được đổi thành PHANCONG$.

- **Khóa chính**, ***Khóa ngoại***

| **NHANVIEN$** | **Đặc tả dữ liệu** | **Lưu trữ thông tin nhân viên** |
|---|---|---|
| **MANV** | VARCHAR2(50 BYTE) | Mã duy nhất của mỗi nhân viên |
| **TENNV** | NVARCHAR2(50 CHAR) | Tên nhân viên |
| **PHAI** | NVARCHAR2(3 CHAR) | Giới tính nhân viên |
| **NGAYSINH** | DATE | Ngày sinh nhân viên |
| **DIACHI** | NVARCHAR2(255 CHAR) | Địa chỉ nhân viên |
| **SODT** | VARCHAR2(15 BYTE) | Số điện thoại nhân viên |
| **LUONG** | VARCHAR2(32 BYTE) | Lương nhân viên |
| **PHUCAP** | VARCHAR2(32 BYTE) | Phụ cấp nhân viên |
| **VAITRO** | NVARCHAR2(20 CHAR) | Vai trò nhân viên |
| **MANQL** | VARCHAR2(50 BYTE) | Mã nhân viên quản lý nhân viên đó |
| ***PHG*** | VARCHAR2(50 BYTE) | Mã phòng của nhân viên đó làm việc |

| **PHANCONG$** | **Đặc tả dữ liệu** | **Lưu trữ thông tin phân công** |
|---|---|---|
| ***MANV*** | VARCHAR2(50 BYTE) | Mã duy nhất của mỗi nhân viên |
| ***MADA*** | VARCHAR2(50 BYTE) | Mã đề án duy nhất |
| **THOIGIAN** | NUMBER | Thời gian thực hiện đề án (giờ) |

| DEAN | Đặc tả dữ liệu | Lưu trữ thông tin đề án |
|---|---|---|
| **MADA** | VARCHAR2(50 BYTE) | Mã đề án duy nhất |
| **TENDA** | NVARCHAR2(255 CHAR) | Tên đề án |
| **NGAYBD** | DATE | Ngày bắt đầu đề án |
| ***PHONG*** | VARCHAR2(50 BYTE) | Mã phòng ban thực hiện đề án |

| PHONGBAN | Đặc tả dữ liệu | Lưu trữ thông tin phòng ban |
|---|---|---|
| **MAPB** | VARCHAR2(50 BYTE) | Mã phòng ban duy nhất |
| **TENPB** | NVARCHAR2(255 CHAR) | Tên phòng ban |
| **TRGPHG** | VARCHAR2(50 BYTE) | Mã của trưởng phòng ban |

## 2.3. Cài đặt các chính sách bảo mật

### 2.3.1. Chính sách DAC

- DAC (Direct Access Control) được sử dụng để phân quyền trên đối tượng dữ liệu cho từng người dùng khác nhau trong hệ thống thông qua các câu lệnh GRANT, REVOKE và DENY.

- DAC trong phân hệ này được dùng để gán các quyền cho các Role và gán Role cho các người dùng trong RBAC.

- Do trong phân hệ có một số thao tác gây ảnh hưởng trực tiếp đến bảng NHANVIEN và PHANCONG nên nhóm đã đổi tên bảng 2 bảng thành NHANVIEN$ và PHANCONG$ sau đó tạo lại 2 View tương ứng là NHANVIEN và PHANCONG để thực thi các chính sách bảo mật trên 2 View đó tránh ảnh hưởng trực tiếp đến 2 bảng chính.

### 2.3.2. Chính sách RBAC

- RBAC (Role-based access control) là một cơ chế phân quyền cho một nhóm người dùng có quyền tương tự nhau thông qua các Role được tạo và cấp Role đó cho người dùng.

- Trong phân hệ này RBAC hoạt động như sau:

+ Hệ thống được chia ra làm 6 Role:

- ROLE_NHANVIEN: dùng để quản lý người dùng có vai trò là Nhân viên và là Role bắt buộc của mỗi người dùng.
- ROLE_TRUONGPHONG: dùng để quản lý người dùng có vai trò là Trưởng phòng.
- ROLE_QLTRUCTIEP: dùng để quản lý người dùng có vai trò là Quản lý trực tiếp.
- ROLE_TAICHINH: dùng để quản lý người dùng có vai trò là Tài chính.
- ROLE_NHANSU: dùng để quản lý người dùng có vai trò là Nhân sự.
- ROLE_TRUONGDA: dùng để quản lý người dùng có vai trò là Trưởng đề án.

+ **CS#1**: Nhân viên chỉ có thể xem thông tin của chính mình trên bảng trên quan hệ NHANVIEN$ và PHANCONG$. ROLE_NHANVIEN có quyền Select trên quan hệ PHONG BAN và có quyền Select trên hai View sau:

- NHANVIEN_SESSION: nhân viên xem thông tin của chính mình trên bảng NHANVIEN$.

```
CREATE OR REPLACE VIEW NHANVIEN_SESSION AS
SELECT *
FROM NHANVIEN$
WHERE MANV = SYS_CONTEXT('USERENV', 'SESSION_USER');
```

- PHANCONG_SESSION: nhân viên xem phân công của chính mình trên bảng PHANCONG$.

```
CREATE OR REPLACE VIEW PHANCONG_SESSION AS
SELECT *
FROM PHANCONG$
WHERE MANV = SYS_CONTEXT('USERENV', 'SESSION_USER');
```

+ **CS#2**: Quản lí trực tiếp có thể xem thông tin của mình và các nhân viên mình quản lí trên bảng NHANVIEN$ trừ thuộc tính LUONG và PHUCAP. ROLE_QLTRUCTIEP có quyền select trên View sau:

- QUANLI_THONGTIN_VIEW: quản lí xem thông tin của mình và các nhân viên do mình quản lí trên bảng NHANVIEN$.

```
CREATE OR REPLACE VIEW QUANLI_THONGTIN_VIEW AS
SELECT NV2.MANV, NV2.TENNV, NV2.PHAI, NV2.NGAYSINH, NV2.DIACHI, NV2.SODT, NV2.VAITRO, NV2.MANQL, NV2.PHG
FROM NHANVIEN$ NV1 JOIN NHANVIEN$ NV2
ON NV2.MANQL=NV1.MANV
WHERE NV1.MANV = SYS_CONTEXT ('userenv', 'session_user');
```

Quản lí trực tiếp  có thể xem các dòng trên bảng PHANCONG$ liên quan mình và các nhân viên do mình quản lí. ROLE_QLTRUCTIEP có quyền select trên View sau:

- QUANLI_PHANCONG_VIEW: quản lí xem phân công của mình và các nhân viên do mình quản lí trên bảng PHANCONG$.

```
CREATE OR REPLACE VIEW QUANLI_PHANCONG_VIEW AS
SELECT PC.MANV,PC.MADA, PC.THOIGIAN
FROM PHANCONG$ PC JOIN NHANVIEN$ NV ON PC.MANV=NV.MANV
WHERE NV.MANQL = SYS_CONTEXT ('userenv', 'session_user') or NV.MANV = SYS_CONTEXT ('userenv', 'session_user')
```

+ **CS#3**: Trưởng phòng có thể xem thông tin của mình và các nhân viên trong phòng ban của mình trên bảng NHANVIEN$ trừ thuộc tính LUONG và PHUCAP. ROLE_TRUONGPHONG có quyền select trên View sau:

- TRUONGPHONG_THONGTIN_VIEW: trưởng phòng xem thông tin của mình và các nhân viên trong phòng của mình trên bảng NHANVIEN$.

```
CREATE OR REPLACE VIEW TRUONGPHONG_THONGTIN_VIEW AS
SELECT NV2.MANV, NV2.TENNV, NV2.PHAI, NV2.NGAYSINH, NV2.DIACHI, NV2.SODT, NV2.VAITRO, NV2.MANQL, NV2.PHG
FROM NHANVIEN$ NV1 JOIN NHANVIEN$ NV2
ON NV2.PHG=NV1.PHG
WHERE NV1.MANV = SYS_CONTEXT ('userenv', 'session_user');
```

Trưởng phòng có thể xem xóa cập nhật trên bảng PHANCONG$ mà mình làm trưởng phòng. ROLE_TRUONGPHONG có quyền select trên View sau:

- TRUONGPHONG_PHANCONG_VIEW: Trưởng phòng được xem phân công của các nhân viên trong phòng của mình.

```
CREATE OR REPLACE VIEW TRUONGPHONG_PHANCONG_VIEW AS
SELECT PC.MANV,PC.MADA, PC.THOIGIAN
FROM PHANCONG$ PC JOIN NHANVIEN$ NV ON PC.MANV=NV.MANV
WHERE NV.MANV = SYS_CONTEXT ('userenv', 'session_user') OR NV.MANQL = SYS_CONTEXT ('userenv', 'session_user');
```

ROLE_TRUONGPHONG có quyền thực hiện các procedure sau:

- INSERT_PHANCONG: Trưởng phòng thêm phân công cho một người trong phòng ban của mình.
- DELETE_PHANCONG: Trưởng phòng xóa một phân công trong phòng ban của mình.
- UPDATE_PHANCONG: Trưởng phòng cập nhật phân công cho một người trong phòng ban của mình.

+ **CS#4**: Nhân viên tài chính được quyền xem thông tin nhân viên và thông tin bảng phân công của toàn bộ nhân viên đồng thời được quyền cập nhật lương và phụ cấp của các nhân viên. ROLE_TAICHINH được quyền Select trên View :

- PHANCONG: Lấy toàn bộ thông tin trên bảng PHANCONG$.

```
---- Tạo view xem trên toàn bộ quan hệ PHANCONG
CREATE OR REPLACE VIEW PHANCONG AS
SELECT *
FROM PHANCONG$;
```

ROLE_TAICHINH được quyền Update trên cột LUONG và PHUCAP của View:

- NHANVIEN: Lấy toàn bộ thông tin trên bảng NHANVIEN$.

```
-- Tạo view xem thuộc tính trên bảng nhân viên
CREATE OR REPLACE VIEW NHANVIEN AS
SELECT *
FROM NHANVIEN$;
```

+ **CS#5**: Nhân sự được quyền cập nhật thông tin tất cả các nhân viên và thông tin tất cả các phòng ban.

ROLE_NHANSU được quyền Insert và Update trên quan hệ PHONGBAN.

ROLE_NHANSU được quyền Select ở trên View:

- NHANVIEN_NHANSU: sử dụng hàm DECODE để che đi cột LUONG và PHUCAP của các nhân viên khác với nhân viên đang thực hiện truy vấn trên quan hệ NHANVIEN$.

```
CREATE OR REPLACE VIEW NHANVIEN_NHANSU
AS
    SELECT MANV, TENNV, PHAI, NGAYSINH, DIACHI, SODT,
    DECODE(MANV, USER, LUONG, NULL) LUONG,
    DECODE(MANV, USER, PHUCAP, NULL) PHUCAP, VAITRO, MANQL, PHG
FROM NHANVIEN$;
```

ROLE_NHANSU được quyền Update tất cả các cột trừ cột LUONG và PHUCAP của View NHANVIEN_NHANSU.

+ **CS#6**: Trưởng đề án có quyền thêm, xóa, cập nhật thông tin của tất cả các đề án.

ROLE_TRUONGDEAN có thể thực hiện INSERT, DELETE, UPDATE trên bảng DEAN (miễn là không vi phạm ràng buộc khóa ngoại).

### 2.3.3. Chính sách VPD

- VPD (Virtual Private Database) là một tính năng cho phép cài đặt các chính sách bảo mật áp dụng trên cơ sở dữ liệu ở mức dòng (row-level) bằng cách chèn thêm các điều kiện khi thực hiện truy vấn trên bảng hay View tương ứng.

- Các chính sách VPD được áp dụng trong phân hệ này:

+ **CS#1**: Người dùng có vai trò Nhân viên chỉ được phép cập nhật trên các trường NGAYSINH, DIACHI, SODT liên quan đến chính nhân viên đó. Thực hiện cài đặt VPD trên View NHANVIEN:

- Với quyền UPDATE có vị từ là MANV = mã nhân viên của chính nhân viên đó và
- Với quyền SELECT có vị từ phụ thuộc vai trò nhân viên nếu là các vai trò khác thì vị từ là MANV = mã nhân viên, còn vai trò tài chính thì có vị từ là 1=1.

```
DROP FUNCTION UPDATE_NV_FUNCTION;
CREATE OR REPLACE FUNCTION UPDATE_NV_FUNCTION (
    P_SCHEMA IN VARCHAR2,
    P_OBJECT IN VARCHAR2) RETURN VARCHAR2
AS
    PREDICATE VARCHAR2(1000);
    MANV VARCHAR(200);
    ROLE_NAME NVARCHAR2(200);
BEGIN

    IF SYS_CONTEXT('USERENV', 'SESSION_USER') = 'U_AD_QLNV' THEN
        RETURN '1=1';
    END IF;

    -- Mỗi user đều có mức quyền thấp nhất là nhân viên nên được quyền select trên view NHANVIEN
    SELECT VAITRO INTO ROLE_NAME FROM U_AD_QLNV.NHANVIEN_SESSION;
    MANV := SYS_CONTEXT('USERENV', 'SESSION_USER');

    IF ROLE_NAME = N'Tài chính' THEN
        PREDICATE := '1=1';
    ELSE
        PREDICATE := 'MANV = '''||MANV||'''';
    END IF;
    RETURN PREDICATE;
END;
```

```
-- Xóa và cài đặt chính sách
BEGIN
    DBMS_RLS.DROP_POLICY(
        OBJECT_SCHEMA => 'U_AD_QLNV',
        OBJECT_NAME => 'NHANVIEN',
        POLICY_NAME => 'UPDATE_NV_POLICY');
END;
/
BEGIN
    DBMS_RLS.ADD_POLICY(
        OBJECT_SCHEMA => 'U_AD_QLNV',
        OBJECT_NAME => 'NHANVIEN',
        POLICY_NAME => 'UPDATE_NV_POLICY',
        POLICY_FUNCTION => 'UPDATE_NV_FUNCTION',
        STATEMENT_TYPES => 'SELECT, UPDATE',
        UPDATE_CHECK => TRUE
    );
END;
/
```

+ Các chính sách còn lại đa phần là dùng View.

### 2.3.4. Chính sách OLS (MAC)

- Oracle Label Security (OLS) là một sản phẩm được hiện thực dựa trên nền tảng công nghệ Virtual Private Database (VPD), cho phép các nhà quản trị điều khiển truy xuất dữ liệu ở mức hàng (row-level) một cách tiện lợi và dễ dàng hơn. Nó điều khiển

việc truy xuất nội dung của các dòng dữ liệu bằng cách so sánh nhãn của hàng dữ liệu với nhãn và quyền của user.

- Khi người dùng nhập vào 1 câu truy vấn SQL, đầu tiên Oracle sẽ kiểm tra DAC để bảo đảm rằng user đó có quyền truy vấn trên bảng được nhắc đến trong câu truy vấn. Kế tiếp Oracle sẽ kiểm tra xem có chính sách VPD nào được áp dụng cho bảng đó không. Nếu có, chuỗi điều kiện của chính sách VPD sẽ được nối thêm vào câu truy vấn gốc, giúp lọc ra được một tập các hàng dữ liệu thỏa điều kiện của VPD. Cuối cùng, Oracle sẽ kiểm tra các nhãn OLS trên mỗi hàng dữ liệu có trong tập trên để xác định những hàng nào mà người dùng có thể truy xuất.

- Các nhãn được chia thành 3 mức độ là Level, Compartment và Group. Chính sách được thiết lập cụ thể như sau:

- Level: Giám đốc (GD) > Trưởng phòng (TP) > Nhân viên (NV)

| LEVEL_NUM | LONG_NAME | SHORT_NAME |
|---|---|---|
| 9000 | GIAM_DOC | GD |
| 7000 | TRUONG_PHONG | TP |
| 4000 | NHAN_VIEN | NV |

- Compartment: Mua bán (MB), Sản xuất (SX), Gia công (GC)

| COM_NUM | LONG_NAME | SHORT_NAME |
|---|---|---|
| 1000 | MUA_BAN | MB |
| 2000 | SAN_XUAT | SX |
| 3000 | GIA_CONG | GC |

- Group: Miền Bắc(B), Miền Trung (T), Miền Nam(N)

| GROUP_NUM | LONG_NAME | SHORT_NAME |
|---|---|---|
| 1000 | MIEN_BAC | B |
| 2000 | MIEN_TRUNG | T |
| 3000 | MIEN_NAM | N |

- Điều chỉnh: Thêm bảng THONGBAO vào cơ sở dữ liệu

| Tên thuộc tính | Kiểu dữ liệu | Đặc tả | Ghi chú |
|---|---|---|---|
| MATB | NUMBER | Mã duy nhất xác định thông báo | Khóa chính, tăng tự động từ 1 |
| NOIDUNG | NVARCHAR2(300) | Nội dung thông báo | |
| NGAYGIO | DATE | Thời gian ra thông báo | |
| CAPBAC | NVARCHAR2(100) | Cấp bậc nhận thông báo | |
| LINHVUC | NVARCHAR2(100) | Lĩnh vực nhận thông báo | |
| CHINHANH | NVARCHAR2(100) | Chi nhánh nhận thông báo | |

- Gán nhãn cho 03 người dùng trong hệ thống:

  - 01 giám đốc có thể đọc được toàn bộ dữ liệu (TONGGIAMDOC): GD:MB,SX,GC:B,T,N
  - 01 trưởng phòng phụ trách lĩnh vực sản xuất miền Nam (TRUONGPHONG_SANXUAT_MIENNAM): TP:SX:N
  - 01 giám đốc phụ trách bất kỳ lĩnh vực nào ở chi nhánh miền Bắc (GIAMDOC_MIENBAC): GD:MB,SX,GC:B

- Kịch bản phát tán dữ liệu:

| STT | Thông báo | Nhãn | USER CÓ THỂ TRUY CẬP |
|---|---|---|---|
| 1 | Thông báo t1 đến tất cả trưởng phòng phụ trách tất cả các lĩnh vực | TP:MB,SX,GC | TONGGIAMDOC, GIAMDOC_MIENBAC |

| | | | |
|---|---|---|---|
| | không phân biệt chi nhánh. | | |
| 2 | Thông báo t2 đến trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung. | TP:SX:T | TONGGIAMDOC |
| 3 | Thông báo t3 đến nhân viên phụ trách lĩnh vực sản xuất ở miền Nam. | NV:SX:N | TONGGIAMDOC, TRUONGPHONG_SANXUAT_MIENNAM |
| 4 | Thông báo t4 đến tất cả nhân viên phụ trách cả hai lĩnh vực mua bán và gia công ở miền Bắc và miền Trung. | NV:MB,GC:B,T | TONGGIAMDOC, GIAMDOC_MIENBAC |
| 5 | Thông báo t5 đến tất cả trưởng phòng phụ trách lĩnh vực sản xuất ở miền Bắc và miền Nam. | TP:SX:B,N | TONGGIAMDOC, GIAMDOC_MIENBAC, TRUONGPHONG_SANXUAT_MIENNAM |

## 2.4. Cài đặt cơ chế mã hóa

### 2.4.1. Mã hóa

- User được quyền thực hiện mã hóa: U_AD_QLNV.

- Mã hóa ở mức ứng dụng, lý do chọn mã hóa ở mức này là vì việc cài đặt mã hóa ở phía cơ sở dữ liệu rất khó khăn.

- Cần thay đổi về cấu trúc lưu trữ dữ liệu: thay kiểu dữ liệu của trường LUONG và PHUCAP từ NUMBER sang VARCHAR2(32 BYTE).

- Thuật toán mã hóa sử dụng là AES256 với độ dài khóa là 256 và mode sử dụng là ECB (IV = 0).

**2.4.2. Cách thức thiết lập khóa:**

- Khóa của mỗi nhân viên sẽ được thiết lập theo quá trình như sau:

1. Trích xuất mã nhân viên.
2. Tạo ra chuỗi khóa bằng cách đan xen các số ở trong mã nhân viên với một chuỗi salt được định sẵn (“Lâm Bích Phước Quân”).
3. Hash chuỗi này bằng thuật toán hàm băm mã hóa SHA256 sẽ thu được khóa của nhân viên.

- Ví dụ với mã nhân viên là NV001 thì chuỗi khóa trước khi hash là:

Lâm0Bích0Phước1Quân

Khi đó, khóa của nhân viên sẽ là:

34ec6862a6dee9fb1e768728c448cf59629a877ce45f03679525ce4b79e65c9d

**2.4.3. Lưu trữ, phân phối và phục hồi khóa:**

- Do khóa chỉ được dùng khi mã hóa/giải mã nên không cần lưu trữ, phân phối và phục hồi khóa.

**2.4.4. Thay khóa đồng loạt sau một thời gian:**

- Thay đổi khóa đồng loạt bằng cách thay đổi công thức tạo ra chuỗi khóa.

## 2.5. Cài đặt chính sách Audit

**2.5.1. Audit những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG.**

```
BEGIN
DBMS_FGA.ADD_POLICY(
object_schema => 'U_AD_QLNV',
object_name => 'PHANCONG$',
policy_name => 'THOIGIAN_PHANCONG',
audit_column => 'THOIGIAN',
statement_types => 'UPDATE',
audit_trail => DBMS_FGA.DB + DBMS_FGA.EXTENDED);
END;
```

- DBMS_FGA.DB+EXTENDED: bản ghi giám sát sẽ được ghi vào bảng SYS.FGA_LOG$ của cơ sở dữ liệu và lưu thêm hai cột SQL Text và SQL Bind.

### 2.5.2. Audit những người đã đọc trên trường LUONG và PHUCAP của người khác.

```
BEGIN
DBMS_FGA.ADD_POLICY(
object_schema => 'U_AD_QLNV',
object_name => 'NHANVIEN$',
policy_name => 'LUONG_PHUCAP_NHANVIEN',
audit_column => 'LUONG,PHUCAP',
audit_condition => q'[SYS_CONTEXT('USERENV', 'SESSION_USER') != MANV]',
statement_types => 'SELECT',
audit_trail => DBMS_FGA.DB + DBMS_FGA.EXTENDED);
END;                                                                    --
```

- Audit_condition: nếu người đang đăng nhập có mã nhân viên khác với mã nhân viên của những người trong bảng thì audit.

### 2.5.3. Một người không thuộc vai trò “Tài chính” nhưng đã cập nhật thành công trên trường LUONG và PHUCAP.

- Lưu lại vai trò của người đang đăng nhập:

```
-- tạo context tên TESTS ĐỂ lưu vai trò của user đang đăng nhập
create context TESTS using U_AD_QLNV.CONTEXT_PACKAGE;
/
-- tạo package có tên CONTEXT_PACKAGE, chứa thủ tục SET_CONTEXT để lấy vaitro
create or replace package CONTEXT_PACKAGE AS
procedure SET_CONTEXT;
end;
```

```
-- thủ tục SET_CONTEXT lấy vaitro
create or replace package body CONTEXT_PACKAGE is
procedure SET_CONTEXT IS
v_manv VARCHAR2(30);
v_vaitro VARCHAR2(30);

begin

    DBMS_SESSION.SET_CONTEXT('TESTS','SETUP','TRUE');
    v_manv := SYS_CONTEXT('USERENV','SESSION_USER');
    begin
        select vaitro into v_vaitro from nhanvien$
        where manv = v_manv;
        DBMS_SESSION.SET_CONTEXT('TESTS','VAITRO',v_vaitro);
    -- nếu username không có trong bảng thì gán rỗng
    exception
        WHEN NO_DATA_FOUND then
        DBMS_SESSION.SET_CONTEXT('TESTS','VAITRO','');
    end;
    DBMS_SESSION.SET_CONTEXT('TESTS','SETUP','FALSE');
end SET_CONTEXT;
end CONTEXT_PACKAGE;
```

```
-- cấp quyền thực thi package với các user khác và tạo 1 public synonym( để khi gọi package chỉ gần ghi CONTEXT_PACKAGE)
grant execute on U_AD_QLNV.CONTEXT_PACKAGE TO PUBLIC;
create or replace public synonym CONTEXT_PACKAGE for U_AD_QLNV.CONTEXT_PACKAGE;

/
--tạo trigger thực hiện context sau khi đăng nhập
create or replace trigger U_AD_QLNV.SET_SECURITY_CONTEXT
after logon on database
begin
U_AD_QLNV.CONTEXT_PACKAGE.SET_CONTEXT;
end;
```

```
BEGIN
  DBMS_FGA.ADD_POLICY(
    object_schema => 'U_AD_QLNV',
    object_name => 'NHANVIEN$',
    policy_name => 'UPDATE_LUONG_PHUCAP_NHANVIEN',
    audit_column => 'LUONG,PHUCAP',
    statement_types => 'UPDATE',
    audit_trail => DBMS_FGA.DB + DBMS_FGA.EXTENDED,
    audit_condition => q'[SYS_CONTEXT('TESTS','VAITRO') != N'Tài chính']'
    );
END;
```

- Audit_condition: Nếu người update cột LUONG hoặc PHUCAP không có vai trò là tài chính thì audit.

### 2.5.4. Xem nhật ký hệ thống

- DBA_FGA_AUDIT_TRAIL là một View trong Oracle Database, lưu trữ thông tin về các hoạt động được ghi lại bởi chính sách FGA (Fine-Grained Auditing).

```
-- Xem bảng audit
SELECT * FROM DBA_FGA_AUDIT_TRAIL;
```

# TÀI LIỆU THAM KHẢO

[1] https://github.com/DAMHONGDUC/phan-he-1/