

BÁO CÁO BÀI TẬP LÝ THUYẾT

Môn: AN TOÀN VÀ BẢO MẬT DỮ LIỆU TRONG HỆ
THỐNG THÔNG TIN



BÁO CÁO ĐỒ ÁN MÔN HỌC

HỆ THỐNG QUẢN LÝ NHÂN VIÊN

GVHD: Lương Vĩ Minh
Tiết Gia Hồng
Phạm Thị Bạch Huệ

MỤC LỤC

THÔNG TIN NHÓM.....	3
I. Phân công công việc.....	3
1. Phân hệ 1	3
2. Phân hệ 2	4
II. Phân tích nghiệp vụ và CSDL	6
1. Phân tích nghiệp vụ	6
2. CSDL	8
III. Chính sách bảo mật	9
1. Chính sách với người dùng có vai trò “Nhân viên”	9
2. Chính sách với người dùng có vai trò “QL trực tiếp”	10
3. Chính sách với người dùng có vai trò “Trưởng Phòng”	11
4. Chính sách với người dùng có vai trò “Tài Chính”	12
5. Chính sách với người dùng có vai trò “Nhân sự”	12
6. Chính sách với người dùng có vai trò “Trưởng đề án”	13
IV. Nhãn OLS	13
1. Tạo OLS policy	13
2. Định nghĩa Label	14
3. Hiện thực hóa nhãn.....	15
4. Áp dụng chính sách OLS.....	16
5. Gán nhãn.....	16
V. Mã hóa	18
1. Đề xuất chiến lược	18
2. Cài đặt.....	18
VI. Auditing	18
a) Chính sách 1: Theo dõi hành vi(SELECT, UPDATE, DELETE, INSERT) của các user trên tất cả table.	18
b) Chính sách 2: Theo dõi các hành vi thực hiện thành công.....	18
c) Chính sách 3: Theo dõi các hành vi thực hiện không thành công.....	18
2. Fine-grained audit	18
a) Chính sách 1: Theo dõi ai đã cập nhật trường Thoi Gian trên bảng phân công.....	18
b) Chính sách 2: Theo dõi ai xem trường Luong,Phu Cap.....	19

c)	<i>Chính sách 3: Theo dõi ai đã cập nhật Lương,Phu Cap</i>	19
VII.	Tài liệu tham khảo.....	20

THÔNG TIN NHÓM

Mã nhóm	MSSV	Họ và tên	Ghi chú
HTTT2 20H3T2-04	20127503	Dương Hiến Lê Hoàng	
	20127423	Đinh Thành Danh	
	20127561	Nguyễn Hoài Mẫn	
	20127649	Nguyễn Trí Trạch	

I. Phân công công việc

1. Phân hệ 1

STT	Công việc	Người thực hiện	Tiến độ (%)
1	Viết script tạo cơ sở dữ liệu và Phát sinh dữ liệu mẫu	Nguyễn Trí Trạch	100%
2	Xem danh sách người dùng trong hệ thống	Nguyễn Hoài Mẫn	100%
3	Thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu	Nguyễn Hoài Mẫn	100%
4	Cho phép tạo mới, xóa, sửa (hiệu chỉnh) user.	Đinh Thành Danh	100%
5	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	Dương Hiến Lê Hoàng	100%

	quyền tinh đến mức cột; quyền insert, delete thì không.		
6	Cho phép thu hồi quyền từ người dùng/ role.	Nguyễn Trí Trách	100%
7	Cho phép kiểm tra quyền của các chủ thể vừa được cấp quyền.	Dương Hiển Lê Hoàng	100%
8	Cho phép chỉnh sửa quyền của user/ role.	Dương Hiển Lê Hoàng	100%

2. Phân hệ 2

STT	Công việc	Người thực hiện	Tiến độ (%)
1	Cài đặt chính sách bảo mật và cấp quyền cho user có vai trò “Nhân viên”	Nguyễn Hoài Mẫn	100%
2	Cài đặt chính sách bảo mật và cấp quyền cho user có vai trò “QL trực tiếp”	Dương Hiển Lê Hoàng	100%
3	Cài đặt chính sách bảo mật và cấp quyền cho user có vai trò “Trưởng phòng”	Dương Hiển Lê Hoàng	100%
4	Cài đặt chính sách bảo mật và cấp quyền cho user có vai trò “Tài chính”	Nguyễn Hoài Mẫn	100%
5	Cài đặt chính sách bảo mật và cấp quyền cho user có vai trò “Nhân sự”	Nguyễn Trí Trách	100%
6	Cài đặt chính sách bảo mật và cấp quyền cho user có vai trò “Trưởng đề án”	Đinh Thành Danh	100%
8	Phân tích chiến lược mã hóa	Đinh Thành Danh	90%

9	Cài đặt mã hóa liên quan đến trường LUONG và PHUCAP	Đinh Thành Danh	40%
10	Phân tích nhân bảo mật OLS	Dương Hiền Lê Hoàng	90%
11	Cài đặt nhân bảo mật OLS	Nguyễn Trí Trạch	70%
12	Cài đặt auditing	Đinh Thành Danh	60%
		Nguyễn Hoài Mẫn	
13	Cài đặt giao diện và chức năng đăng nhập	Nguyễn Hoài Mẫn	100%
16	Cài đặt chức năng phần mềm liên quan đến Nhân viên	Nguyễn Hoài Mẫn	100%
17	Cài đặt chức năng phần mềm liên quan đến Nhân sự	Nguyễn Trí Trạch	100%
18	Cài đặt chức năng phần mềm liên quan đến Tài chính	Nguyễn Hoài Mẫn	100%
19	Cài đặt chức năng phần mềm liên quan đến Trưởng đề án	Đinh Thành Danh	100%
20	Cài đặt chức năng phần mềm liên quan đến Trưởng phòng	Dương Hiền Lê Hoàng	100%
21	Cài đặt chức năng phần mềm liên quan đến Quản lý trực tiếp	Dương Hiền Lê Hoàng	100%
22	Cài đặt giao diện Auditting	Đinh Thành Danh	100%

II. Phân tích nghiệp vụ và CSDL

1. Phân tích nghiệp vụ

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 (TENN), 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

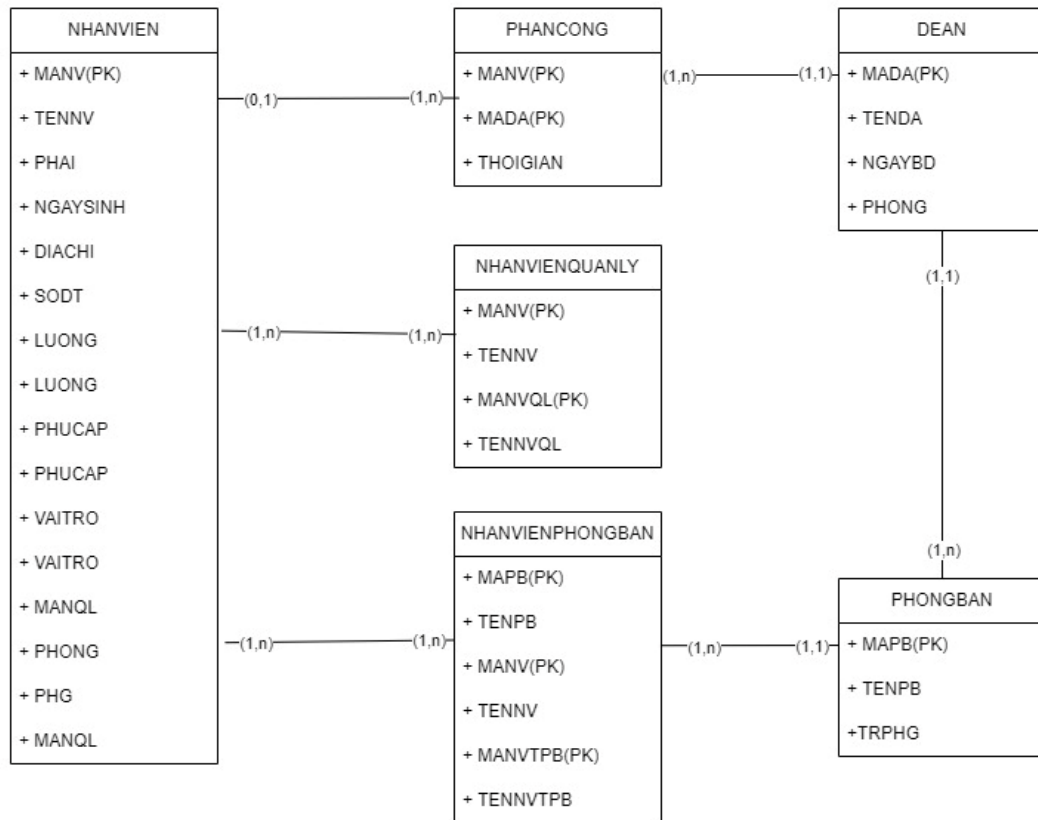
NHANVIENQUANLY (MANV, TENNV, MANVQL, TENNVQL)

Mỗi mỗi nhân viên có MANV và có thêm một MANVQL để biết được nhân viên quản lý trực tiếp nào quản lý mình

NHANVIENPHONGBAN(MAPB, TENPB, MANV, TENNV, MANVTPB, TENNVTPB)

Mỗi nhân viên có MAPB, MANV, MANVTPB, để biết được nhân viên đó ở phòng ban nào và được quản lý bởi nhân viên trưởng phòng ban nào

2. CSDL



III. Chính sách bảo mật

1. Chính sách với người dùng có vai trò “Nhân viên”

Yêu cầu	Cách thực hiện
Có quyền xem tất cả các thuộc tính trên quan hệ NHANVIEN và PHANCONG liên quan đến chính nhân viên đó.	<ul style="list-style-type: none">- Tạo view NHANVIEN_V view này chỉ được lấy thông tin của chính nhân viên đăng nhập vào trên bảng NHANVIEN- GRANT SELECT ON NHANVIEN_V TO Nhan_Vien- Tạo view PHANCONG_V view này chỉ được lấy thông tin của chính nhân viên đăng nhập vào trên bảng PHANCONG- GRANT SELECT ON PHANCONG_V TO Nhan_Vien
Có thể sửa trên các thuộc tính NGAYSINH, DIACHI, SODT liên quan đến chính nhân viên đó	<ul style="list-style-type: none">- Tạo view NHANVIENUPDATE_V view này chỉ được lấy thông tin của chính nhân viên đăng nhập vào trên bảng NHANVIEN- GRANT UPDATE ON NHANVIEN_V TO Nhan_Vien
Có thể xem dữ liệu của toàn bộ quan hệ PHONGBAN và DEAN.	<ul style="list-style-type: none">- GRANT SELECT ON PHONGBAN TO Nhan_Vien;- GRANT SELECT ON DEAN TO Nhan_Vien;

2. Chính sách với người dùng có vai trò “QL trực tiếp”

Yêu cầu	Cách thực hiện
Có quyền như là một nhân viên thông thường (vai trò “Nhân viên”).	GRANT Nhan_Vien TO QL_Truc_Tiep
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.	<ul style="list-style-type: none"> - Tạo view NHANVIENQUANLY_V để hạn chế nhân viên quản lý chỉ được xem tất cả thuộc tính trừ LUONG và PHUCAP - Tạo chính sách VPD áp dụng lên bảng view NHANVIENQUANLY_V để chỉ cho phép nhân viên quản lý trực tiếp xem được nhân viên mình quản lý mà thôi - GRANT SELECT ON NHANVIENQUANLY_V TO QL_Truc_Tiep;
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.	<ul style="list-style-type: none"> - Tạo view NHANVIENQLPHANCONG_V để xem được thông tin nhân viên được phân công - Tạo chính sách VPD áp dụng lên bảng view NHANVIENQLPHANCONG_V để chỉ cho phép nhân viên quản lý trực tiếp xem được nhân viên mình quản lý mà thôi - GRANT SELECT ON NHANVIENQLPHANCONG_V TO QL_Truc_Tiep;

3. Chính sách với người dùng có vai trò “Trưởng Phòng”

Yêu cầu	Cách thực hiện
Có quyền như là một nhân viên thông thường (vai trò “Nhân viên”).	GRANT Nhan_Vien TO Truong_Phong
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.	<ul style="list-style-type: none"> - Tạo view NHANVIENPHONGBAN_V để hạn chế nhân viên quản lý chỉ được xem tất cả thuộc tính trừ LUONG và PHUCAP - Tạo chính sách VPD áp dụng lên bảng view NHANVIENPHONGBAN_V để chỉ cho phép nhân viên trưởng phòng xem được nhân viên phòng ban của mình - GRANT SELECT ON NHANVIENQUANLY_V TO Truong_Phong
Có thể thêm, xóa, cập nhật trên quan hệ PHANCONG liên quan đến các nhân viên thuộc phòng ban mà T làm trưởng phòng.	<ul style="list-style-type: none"> - Tạo view NHANVIENPBPHANCONG_V để xem được thông tin nhân viên được phân công - Tạo chính sách VPD áp dụng lên bảng view NHANVIENPBPHANCONG_V để chỉ cho phép nhân viên trưởng phòng thêm, xóa, cập nhật được nhân viên phòng ban của mình - GRANT SELECT, UPDATE, DELETE, INSERT ON NHANVIENPBPHANCONG_V TO Truong_Phong;

4. Chính sách với người dùng có vai trò “Tài Chính”

Yêu cầu	Cách thực hiện
Có quyền như là một nhân viên thông thường (vai trò “Nhân viên”).	GRANT Nhan_Vien TO Tai_Chinh
Xem trên toàn bộ quan hệ NHANVIEN và PHANCONG, có thể sửa trên thuộc tính LUONG và PHUCAP (thừa hành ban giám đốc).	<ul style="list-style-type: none"> - Tạo view TC_NHANVIEN để xem thông tin nhân viên trên bảng NHANVIEN - Tạo view TC_PHANCONG TO để xem thông tin nhân viên trên bảng PHANCONG - GRANT SELECT ON TC_NHANVIEN TO Tai_Chinh; - GRANT SELECT ON TC_PHANCONG TO Tai_Chinh; - Tạo chính sách VPD để chỉ cho phép nhân viên tài chính chỉnh sửa trường LUONJG và PHUCAP

5. Chính sách với người dùng có vai trò “Nhân sự”

Yêu cầu	Cách thực hiện
Có quyền như là một nhân viên thông thường (vai trò “Nhân viên”).	GRANT Nhan_Vien TO Nhan_Su;
Được quyền thêm, cập nhật trên quan hệ PHONGBAN.	CREATE OR REPLACE VIEW PHONGBAN_VIEW AS SELECT MAPB, TENPB, TRPHG FROM PHONGBAN; GRANT SELECT, INSERT, UPDATE ON PHONGBAN_VIEW TO Nhan_Su;
	CREATE VIEW NHANVIENNHANSU_V AS

Thêm dữ liệu trong quan hệ nhân viên	SELECT MANV, TENNV, PHAI, NGAYSINH, DIACHI, SODT, VAITRO FROM NHANVIEN; GRANT SELECT, INSERT ON NHANVIENNHANSU_V TO Nhan_Su
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	CREATE OR REPLACE VIEW NHANVIEN_VIEW_luong_phucap_null AS SELECT MANV, TENNV, PHAI, NGAYSINH, DIACHI, SODT, LUONG, PHUCAP, VAITRO, MANQL, PHG FROM NHANVIEN WHERE LUONG IS NULL OR PHUCAP IS NULL; GRANT SELECT, UPDATE ON NHANVIEN_VIEW_luong_phucap_null TO Nhan_Su;

6. Chính sách với người dùng có vai trò “Trưởng đề án”

Yêu cầu	Cách thực hiện
Có quyền như là một nhân viên thông thường (vai trò “Nhân viên”).	GRANT Nhan_Vien TO Truong_De_An;
Được quyền thêm, xóa, cập nhật trên quan hệ ĐEAN.	GRANT INSERT, DELETE, UPDATE ON TDA_DEAN TO Truong_De_An;

IV. Nhãn OLS

1. Tạo OLS policy

Đầu tiên, ta tạo chính sách OLS (OLS policy):

- Đối tượng dữ liệu cần được bảo vệ: bảng
- Định nghĩa cột chứa nhãn: ROWLABEL
- Tạo policy: Gọi procedure SA_SYSDBA.CREATE_POLICY với policy_name là ESBD, column_name là ROWLABEL.
- Oracle tự động tạo role ESBD_DBA tương ứng với vai trò quản trị OLS. Thực hiện cấp role này cho schema có vai trò quản trị tương ứng.

- Thực hiện cấp các quyền cần thiết cho schema trên:
 - Quyền tạo các thành phần của nhãn hợp lệ
 - Quyền tạo nhãn hợp lệ
 - Quyền gán nhãn cho user
 - Quyền chuyển đổi một chuỗi ký tự sang thể hiện dạng số của nhãn

2. Định nghĩa Label

Nhãn được yêu cầu gồm 3 thành phần: Level, Compartment, Group

Định nghĩa thành phần level: Level của nhãn là mức độ nhạy cảm của dữ liệu là Sử dụng 3 cấp bậc của NHANVIEN để làm 3 level của nhãn:

Number	Long name	Short name
1000	Giám đốc	GD
3000	Trưởng phòng	TP
5000	Nhân viên	NV

Gọi procedure SA_COMPONENTS.CREATE_LEVEL để tạo lần lượt 3 level của nhãn.

Định nghĩa thành phần compartment: Compartment của nhãn được định nghĩa theo thuộc tính Tuyến của quan hệ NHANVIEN(sự phân chia theo chuyên môn, kỹ thuật)

Number	Long name	Short name
10	Gia công	GIACG
50	Sản xuất	SANX
250	Mua bán	MUAB

Gọi procedure SA_COMPONENTS.CREATE_COMPARTMENT để tạo lần lượt 3 compartment của nhãn (3 compartment giống nhau ở cả 3 level)

Định nghĩa thành phần group: Group của nhãn được định nghĩa theo thuộc tính Vùng của quan hệ CSYT (sự phân chia theo vị trí địa lý)

Number	Long name	Short name
2000	Miền Bắc	MB
4000	Miền Trung	MT
6000	Miền Nam	MN

Gọi procedure SA_COMPONENTS.CREATE_GROUP để tạo lần lượt 3 group của nhãn.

3. Hiện thực hóa nhãn

Tạo label_tag:

Vai trò/Chức vụ	Label	Label_Tag
Giám đốc	GD: GIACG, SANX, MUAB: MB, MT, MN	100
Trưởng phòng phụ trách lĩnh vực sản xuất miền Nam	TP: SANX: MN	200
Giám đốc phụ trách bất kỳ lĩnh vực nào ở chi nhánh miền Bắc	GD: GIACG, SANX, MUAB: MB	300
Trưởng phòng phụ trách tất cả các lĩnh vực không phân biệt chi nhánh.	TP: GIACG, SANX, MUAB: MB, MT, MN	400
Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung.	TP: SANX: MT	500

Gọi procedure SA_COMPONENTS.CREATE_LABEL, truyền vào các tham số tương ứng với bảng trên.

4. Áp dụng chính sách OLS

Dựa vào các phân tích đã nêu, chúng ta bắt đầu áp dụng chính sách OLS lần lượt vào các đối tượng dữ liệu cần bảo vệ

Áp dụng policy vào bảng NHANVIEN bằng cách thực thi procedure APPLY_TABLE_POLICY trong package SA_POLICY_ADMIN.

Gọi thực thi với tham số table_options là NO_CONTROL, điều này khiến cho DBMS ngăn chặn mọi hành vi truy cập vào bảng trước khi các nhãn được gán (vì dữ liệu chưa được gán nhãn nên user không có quyền đọc/ghi trên dữ liệu)

Có 3 cách để gán nhãn cho dữ liệu:

- Cách 1: làm thủ công bằng INSERT/UPDATE.
- Cách 2: dùng LABEL_DEFAULT.
- Cách 3: dùng procedure/function/trigger để cập nhật tự động.

Ở ngữ cảnh này, sử dụng cách 1

- Lúc này, schema hiện tại có quyền tạo các thành phần label cũng như label nhưng không có quyền truy cập, chỉnh sửa trên bảng NHANVIEN.
- Sử dụng cơ chế DAC, cấp quyền cho schema hiện tại được SELECT, INSERT, UPDATE trên bảng NHANVIEN
- Dùng lệnh INSERT, UPDATE để gán lần lượt các nhãn cho từng dòng dữ liệu.

5. Gán nhãn

Phân quyền

Loại user	Phân quyền	Max_read_label	Quyền
Giám đốc	Tất cả giám đốc	GD: GIACG, SANX, MUAB: MB, MT, MN	Đọc được toàn bộ dữ liệu
	Giám đốc phụ trách bất kỳ lĩnh vực nào ở chi nhánh miền Bắc	GD: GIACG, SANX, MUAB: MB	Có thể đọc được toàn bộ dữ liệu theo đúng cấp bậc và không phân biệt lĩnh vực

Trưởng Phòng	Trưởng phòng phụ trách lĩnh vực sản xuất miền Nam	TP: SANX: MN	Đọc được dữ liệu cho trưởng phòng thuộc lĩnh vực sản xuất ở miền nam
	Trưởng phòng phụ trách tất cả các lĩnh vực không phân biệt chi nhánh.	TP: GIACG, SANX, MUAB: MB, MT, MN	Đọc được dữ liệu của tất cả trưởng phòng.
	Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung.	TP: SANX: MT	Đọc được dữ liệu cho trưởng phòng thuộc lĩnh vực sản xuất ở miền trung

Gọi procedure `SA_USER_ADMIN.SET_USER_LABELS` để thêm lần lượt các nhãn user vào như bảng trên

“Gỡ” policy đang cài với tùy chọn `NO_CONTROL` ở hiện tại và cài lại policy với tùy chọn `READ_CONTROL` để hạn chế việc đọc trên bảng

Dùng procedure `SA_USER_ADMIN.SET_USER_PRIVS` để gán nhãn cho user với các tùy chọn quyền khác nhau (`PROFILE ACCESS`, `READ`, `WRITE`, `FULL`)

Kịch bản minh họa phát tán dữ liệu:

Giả định quan hệ `NHANVIEN` có các dòng như sau:

MANV	TENV	PHAI	NGAY SINH	CHI NHANH	SODT	LUONG	PH U CAP	VAI TRO	LINH VUC	ROWLABEL
NV011	Đức	Nam	1989-10-1	Miền Bắc	09900	9000	1000	Trưởng phòng	Sản Xuất	TP: SANX: MN
NV029	Ngân	Nữ	1998-3-1	Miền Trung	02913	2000	3000	Trưởng phòng	Sản Xuất	TP: SANX: MT

- Dòng dữ liệu `MANV = NV011` phát tán đến giám đốc, giám đốc phụ trách bất kỳ lĩnh vực nào ở chi nhánh miền Bắc, Trưởng phòng phụ trách tất cả các lĩnh vực không phân biệt chi nhánh.
- Dòng dữ liệu `MANV = NV029` phát tán đến giám đốc, giám đốc phụ trách bất kỳ lĩnh vực nào ở chi nhánh miền Bắc, Trưởng phòng phụ trách tất cả các lĩnh

vực không phân biệt chi nhánh, Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung.

V. Mã hóa

1. Đề xuất chiến lược

a) Mục đích

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

b) Phương pháp

- + User có vai trò mã hóa: QUANLY
- + Mức mã hóa: Mã hóa mức dữ liệu
- + Thay đổi về cấu trúc dữ liệu: KHÔNG
- + Phương pháp quản lý khóa: Khóa sẽ được lưu trữ trên cơ sở dữ liệu. Việc mã hóa và giải mã cũng sẽ được thực hiện trên cơ sở dữ liệu.

2. Cài đặt

VI. Auditing

Để kích hoạt audit, DBA hoặc người dùng giữ vai trò đứng đầu hệ thống phải chạy dòng lệnh sau:

```
ALTER SYSTEM SET audit_trail = DB SCOPE = SPFILE
```

1. Standard audit

- a) Chính sách 1: Theo dõi hành vi(SELECT, UPDATE, DELETE, INSERT) của các user trên tất cả table.
- b) Chính sách 2: Theo dõi các hành vi thực hiện thành công.
- c) Chính sách 3: Theo dõi các hành vi thực hiện không thành công.

2. Fine-grained audit

- a) *Chính sách 1*: Theo dõi ai đã cập nhật trường Thoi Gian trên bảng phân công

```
BEGIN
dbms_fga.ADD_POLICY (
    OBJECT_SCHEMA => 'QUANLY',
```

```

OBJECT_NAME => 'PHANCONG', --Bang Phan cong hoac View Phan cong
POLICY_NAME => 'AUDIT_UPDATE_THOIGIAN_PHANCONG',
AUDIT_COLUMN => 'THOIGIAN',
STATEMENT_TYPES => 'UPDATE',
ENABLE => TRUE);
END;

```

b) *Chính sách 2: Theo dõi ai xem trường Lương,Phu Cap*

```

BEGIN
  dbms_fga.ADD_POLICY (
    OBJECT_SCHEMA => 'QUANLY',
    OBJECT_NAME => 'NHANVIEN',
    POLICY_NAME => 'AUDIT_SELECT_LUONG_PHUCAP',
    AUDIT_COLUMN => 'LUONG, PHUCAP',
    AUDIT_CONDITION => 'USERNAME <>
SYS_CONTEXT('USERENV','SESSION_USER')',
    STATEMENT_TYPES => 'SELECT',
    ENABLE => TRUE);
END;

```

c) *Chính sách 3: Theo dõi ai đã cập nhật Lương,Phu Cap*

```

BEGIN
  dbms_fga.ADD_POLICY (
    OBJECT_SCHEMA => 'QUANLY',
    OBJECT_NAME => 'NHANVIEN',
    POLICY_NAME => 'AUDIT_UPDATE_LUONG_PHUCAP',
    AUDIT_COLUMN => 'LUONG, PHUCAP',
    AUDIT_CONDITION => 'VAITRO <> ''Tai_Chinh''',
    STATEMENT_TYPES => 'UPDATE',
    ENABLE => TRUE);
END;

```

Theo dõi các hành vi thành công

```
AUDIT ALL WHENEVER SUCCESSFUL;
```

Theo dõi các hành vi không thành công

```
AUDIT ALL WHENEVER NOT SUCCESSFUL;
```

Tạo policy của check khi ai xem Lương, Phu Cap

```

BEGIN
  DBMS_FGA.ADD_POLICY(
    object_schema => 'QUANLY',
    object_name => 'NHANVIEN',
    policy_name => 'CHECK_LUONG_PHUCAP_ON_NHANVIEN',
    enable => TRUE,
    statement_types => 'SELECT',
    audit_column => 'LUONG, PHUCAP',
    audit_trail => DBMS_FGA.DB + DBMS_FGA.EXTENDED,

```

```

        audit_condition => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') !=
        USERNAME');
END;

```







Tạo policy khi ai đó update trên Luong, Phu Cap

```

BEGIN
    DBMS_FGA.ADD_POLICY(
        object_schema => 'QUANLY',
        object_name    => 'NHANVIEN',
        policy_name     => 'CHECK_UPDATE_ON_LUONG_PHUCAP',
        enable          => TRUE,
        statement_types => 'UPDATE',
        audit_column    => 'LUONG, PHUCAP',
        audit_trail      => DBMS_FGA.DB + DBMS_FGA.EXTENDED,
        audit_condition => 'SYS_CONTEXT(''USERENV'', ''SESSION_USER'') NOT IN
        (SELECT grantee FROM dba_role_privs WHERE granted_role = ''Tai_Chinh'')');

```

VII. Tài liệu tham khảo

-  Tài liệu của moudle môn học
-  Cách kết nối Oracle với Winform C#: [Xem tại đây](#)
-  Tài nguyên youtube: [Xem tại đây](#)
-  Tài nguyên github: [Link 1](#), [Link 2](#), [Link 3](#).
-  Tài liệu của Oracle: [Xem tại đây](#)
-  Tài liệu auditing: [Link 1](#), [Link 2](#)