**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**



A picture containing text, map

Description automatically generated

**BÁO CÁO ĐỒ ÁN CUỐI KỲ**

**BỘ MÔN: AN TOÀN BẢO MẬT HỆ THỐNG THÔNG TIN**

**CHỦ ĐỀ: QUẢN LÝ QUÁ TRÌNH BÌNH BẦU TÍN NHIỆM**

**Giảng viên**: Phạm Thị Bạch Huệ

**Sinh viên**: 1612642 Tống Thị Cam Thảo

1612684 Trần Hồ Như Thủy

**05/07/2019**

MỤC LỤC

[**I.** **THÔNG TIN THÀNH VIÊN:** 3](#_Toc13427547)

[**II.** **PHÂN CÔNG VÀ ĐÁNH GIÁ CÔNG VIỆC:** 3](#_Toc13427550)

[**III.** **MÔ TẢ ĐỒ ÁN** 3](#_Toc13427551)

[**IV.** **BÁO CÁO ĐỒ ÁN** 3](#_Toc13427552)

[PHẦN 1: HỆ THỐNG DÀNH CHO NGƯỜI QUẢN TRỊ VIÊN: 3](#_Toc13427553)

[**1.** **Phần giao diện:** 3](#_Toc13427554)

[**2.** **Yêu cầu dành cho Quản trị viên:** 6](#_Toc13427555)

[PHẦN 2: THỰC HIỆN CÁC CHÍNH SÁCH BẢO MẬT 9](#_Toc13427556)

[**1.** **Mô hình dữ liệu quan hệ:** 9](#_Toc13427557)

[**2.** **Hệ thống User/ Role/ Table:** 9](#_Toc13427558)

[**3.** **Các chính sách bảo mật** 10](#_Toc13427559)

[**4.** **Phân tích các yêu cầu bảo mật:** 11](#_Toc13427560)

[**5.** **Audit:** 15](#_Toc13427561)

[**6.** **Mã hóa:** 18](#_Toc13427562)

1. **THÔNG TIN THÀNH VIÊN:**

|  |  |  |
| --- | --- | --- |
| **Nhóm 29:** |  |  |
| **MSSV** | **Họ tên** | **Email** |
| 1612642 | Tống Thị Cam Thảo | camthao98dl@gmail.com |
| 1612684 | Trần Hồ Như Thủy | thnthuy@gmail.com |

1. **PHÂN CÔNG VÀ ĐÁNH GIÁ CÔNG VIỆC:**

|  |  |  |
| --- | --- | --- |
| **CÔNG VIỆC** | **NGƯỜI THỰC HIỆN** | **MỨC ĐỘ HOÀN THÀNH** |
| RBAC + DAC | Cam Thảo | 90% |
| VPD | Như Thủy | 80% |
| MAC (OLS) | Cam Thảo |  |
| Mã hóa | Cam Thảo | 90% |
| Audit | Như Thủy | 90% |
| Giao diện role/user/table | Như Thủy | 100% |
| Giao diện Auit | Như Thủy | 100% |
| Giao diện Mã hóa | Cam Thảo | 90% |
| Báo cáo | Cả nhóm | 90% |

1. **MÔ TẢ ĐỒ ÁN**

Đồ án xây dựng ứng dụng quản lý quá trình bình bầu tín nhiệm có 2 phân hệ.

**Phân hệ 1**: Dành cho người quản trị người dùng và điều khiển truy cập. Tạo các user, role, cấp quyền và thu quyền, xem quyền được cấp của một đối tượng cụ thể, xem lịch sử Audit, …

**Phân hệ 2**: Cấp quyền truy cập cho từng đối tượng, thiết lập cơ chế, chính sách bảo mật.

1. **BÁO CÁO ĐỒ ÁN**

## PHẦN 1: HỆ THỐNG DÀNH CHO NGƯỜI QUẢN TRỊ VIÊN:

1. **Phần giao diện:**

***Giao diện chính dành cho người quản trị:***

A screenshot of a cell phone

Description automatically generated

***Giao diện admin Xem User, Role, Table:***

A screenshot of a cell phone

Description automatically generated

***Giao diện admin Xem thông tin đối tượng cụ thể:***

A screenshot of a cell phone

Description automatically generated

***Giao diện admin Cấp/Thu lại quyền:***

A screenshot of a social media post

Description automatically generated

***Giao diện Thêm user:***

A screenshot of a cell phone

Description automatically generated

1. **Yêu cầu dành cho Quản trị viên:**
   1. Xem danh sách các đối tượng hiện có trên CSDL (user, role, table):

***Đối tượng trên User***



A screenshot of a cell phone

Description automatically generated

***Đối tượng trên Role***

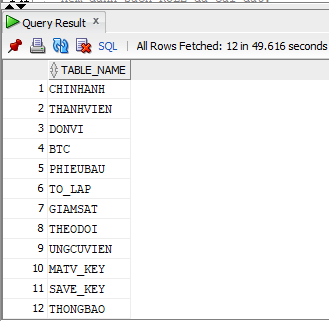


A screenshot of a cell phone

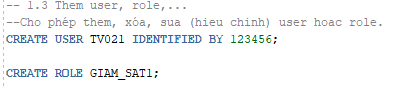
Description automatically generated

***Đối tượng trên Table***





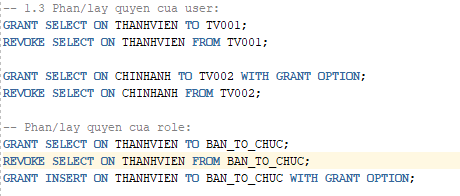
* 1. **Thêm mới đối tượng (user, role, table, …):**



**A screenshot of a cell phone

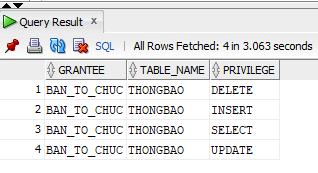
Description automatically generated**

* 1. **Phân quyền và lấy lại quyền của role/ user:**



* 1. **Xem quyền của một đối tượng cụ thể:**





## PHẦN 2: THỰC HIỆN CÁC CHÍNH SÁCH BẢO MẬT

1. **Mô hình dữ liệu quan hệ:**

**CHINHANH** (MACHINHANH, TENCHINHANH)

**THANHVIEN** (MA\_THANHVIEN, HOTEN, GIOITINH, QUEQUAN, NAMSINH, QUOCTICH, DC\_THUONGTRU, DC\_TAMTRU, DONVI, CHINHANH, CONGTAC, TAMNGHI, LUONG)

**DONVI** (MA\_DONVI, TENDONVI, TRUONGDONVI)

**BTC** (ID\_BTC, HOTEN, NAMSINH, GIOITINH)

**PHIEUBAU** (MA\_THANHVIEN, UCV1, UCV2, UCV3)

**TO\_LAP** (ID\_TOLAP, HOTEN, NAMSINH, GIOITINH, DONVI)

**GIAMSAT** (ID\_GIAMSAT, HOTEN, NAMSINH, GIOITINH)

**THONGBAO** (NOIDUNG, LOAITB, COLUMN\_OLS)

**THEODOI** (ID\_THEODOI, HOTEN, NAMSINH, GIOITINH)

**UNGCUVIEN** (MA\_UCV, HOTEN, NAMSINH, CHUCVU, KHOA)

1. **Hệ thống User/ Role/ Table:**

***Các user:***

* Tạo 20 user từ 20 dòng dữ liệu trong bảng THANHVIEN
* Có 2 loại người dùng chính: Bộ phận Ban tổ chức và các bộ phận khác. Tương ứng với các bộ phận sẽ có các loại người dùng khác nhau. Từ đó áp dụng cơ chế RBAC để xây dựng các role người dùng.

***Các role:***

ROLE THANHVIEN;

ROLE BAN\_TO\_CHUC;

ROLE TRUONG\_BTC;

ROLE TO\_LAP;

ROLE THEO\_DOI;

ROLE GIAM\_SAT;

ROLE UNG\_CU\_VIEN;

1. **Các chính sách bảo mật**

***Trưởng ban tổ chức***

Trưởng ban tổ chức có quyền thêm, xem, xóa, sửa bảng Ứng cử viên 🡪 Sử dụng RBAC (DAC)

***Ban tổ chức***

Người thuộc ban tổ chức bình bầu chỉ có thể xem, xóa, sửa thông tin trong danh sách ứng cử viên, những người thuộc tổ lập danh sách người đi bầu, tổ theo dõi kết quả và tổ giám sát. 🡪 Sử dụng RBAC (DAC)

***Tổ theo dõi kết quả:***

Tổ theo dõi kết quả được xem danh sách tất cả những người đi bầu thuộc tất cả các đơn vị và chỉ có thể biết được ai trong danh sách những người đi bầu đã hoặc chưa đi bầu, tuy nhiên họ không biết được mỗi người đã bình bầu cho những ứng viên nào. Những người này có thể theo dõi số lần bình bầu cho từng ứng cử viên. 🡪 Sử dụng RBAC (DAC)

***Giám sát***

Bộ phận giám sát được toàn quyền xem thông tin trên ứng dụng, nhưng không được thay đổi bất cứ thông tin gì. 🡪 RBAC (DAC)

RBAC là điều khiển truy cập trên role (nâng cấp của DAC trong các trường hợp phải phân quyền cho quá nhiều người dùng)

DAC là điều khiển việc truy cập của chủ thể vào đối tượng thông qua định danh của chủ thể và các luật cho trước. DAC phân quyền tới cụ thể từng user.

***Thành viên***

Thành viên chỉ được xem lương của chính mình 🡪 Sử dụng VPD

1. **Phân tích các yêu cầu bảo mật:**

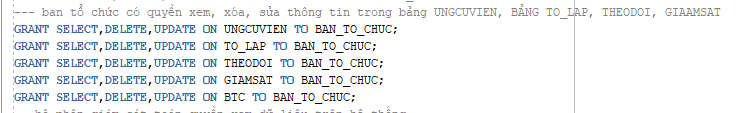
***Trưởng ban tổ chức***

Trưởng ban tổ chức có quyền thêm, xem, xóa, sửa bảng Ứng cử viên 🡪 RBAC (DAC)



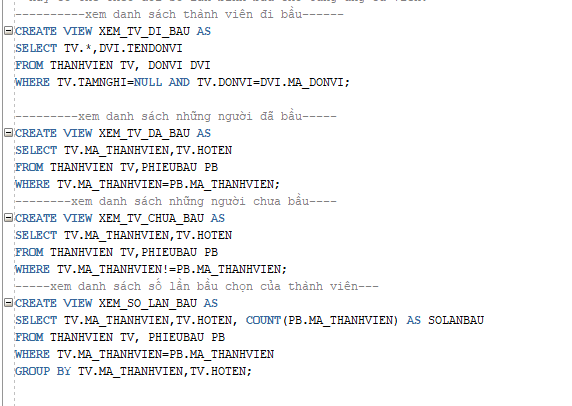
***Ban tổ chức***

Người thuộc ban tổ chức bình bầu chỉ có thể xem, xóa, sửa thông tin trong danh sách ứng cử viên, những người thuộc tổ lập danh sách người đi bầu, tổ theo dõi kết quả và tổ giám sát. 🡪 RBAC (DAC)



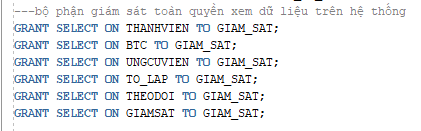
***Tổ theo dõi kết quả:***

Tổ theo dõi kết quả được xem danh sách tất cả những người đi bầu thuộc tất cả các đơn vị và chỉ có thể biết được ai trong danh sách những người đi bầu đã hoặc chưa đi bầu, tuy nhiên họ không biết được mỗi người đã bình bầu cho những ứng viên nào. Những người này có thể theo dõi số lần bình bầu cho từng ứng cử viên. 🡪 RBAC (DAC)



***Giám sát***

Bộ phận giám sát được toàn quyền xem thông tin trên ứng dụng, nhưng không được thay đổi bất cứ thông tin gì. 🡪 RBAC (DAC)



***Thành viên***

* Thành viên chỉ được xem lương của chính mình 🡪 Sử dụng VPD

A screenshot of a social media post

Description automatically generated  
**🡪 Kết quả sử dụng VPD:** chỉ có TV001 mới có thể xem được lương của chính mình:

A screenshot of a social media post

Description automatically generated

* Chỉ thành viên mới xem được kết quả mã hóa địa chỉ CONGTAC của mình 🡪 Sử dụng VPD:



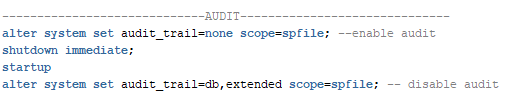
1. **Audit:**

- ***Khái niệm***: Audit là hoạt động theo dõi và ghi lại nhật ký các hoạt động, thao tác của người dùng trên cơ sở dữ liệu

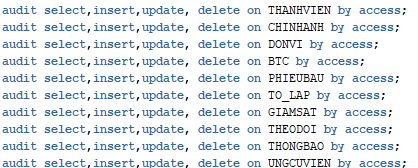
- ***Ngữ cảnh***: Check nhật ký các hoạt động liên quan đến **thêm/xóa/sửa/chọn** trên tất cả các bảng thuộc lược đồ cơ sở dữ liệu

- ***Script thực hiện:***

***Kích hoạt chức năng giám sát:***



***Giám sát mọi câu lệnh thêm/xóa/sửa/chọn trên các bảng:***



***Kiểm tra dữ liệu đã ghi nhận:***



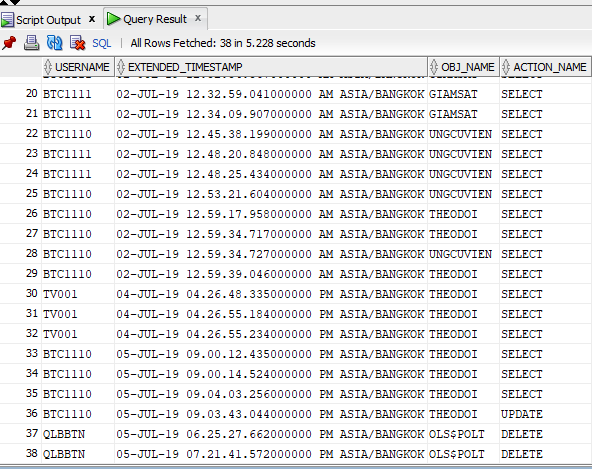
***Giám sát câu truy vấn thành công****:*



***Giám sát câu truy vấn báo lỗi:***



* **Kết quả Audit:**



***Giao diện Xem lịch sử Audit:***

A screenshot of a cell phone

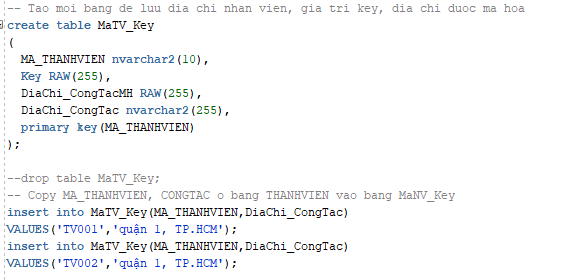
Description automatically generated

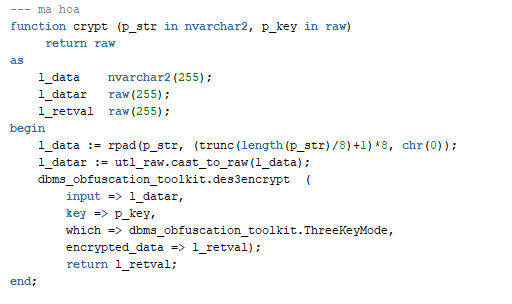
1. **Mã hóa:**

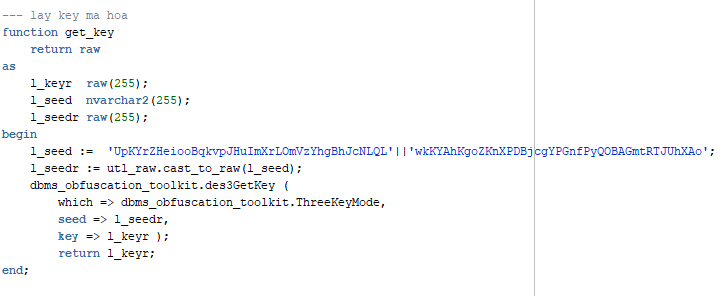
- ***Khái niệm***: Mã hóa là quá trình biến đổi dữ liệu từ dạng văn bản bình thường sang dạng mã (không có nghĩa). Từ dạng mã muốn chuyển về cần phải giải mã

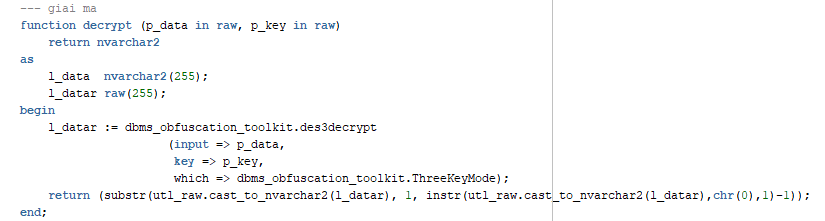
- ***Ngữ cảnh***: Chỉ có các đối tượng được cấp quyền mới xem được nơi công tác của thành viên.

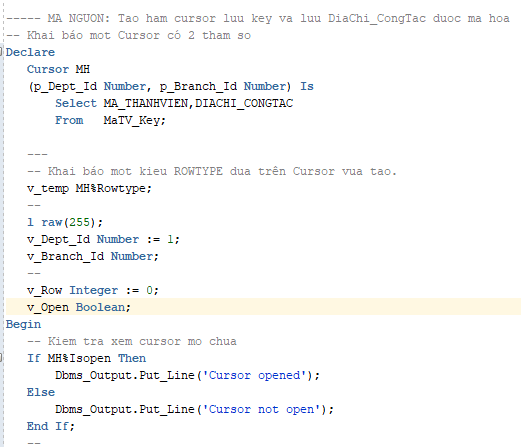
- ***Script thực hiện:***

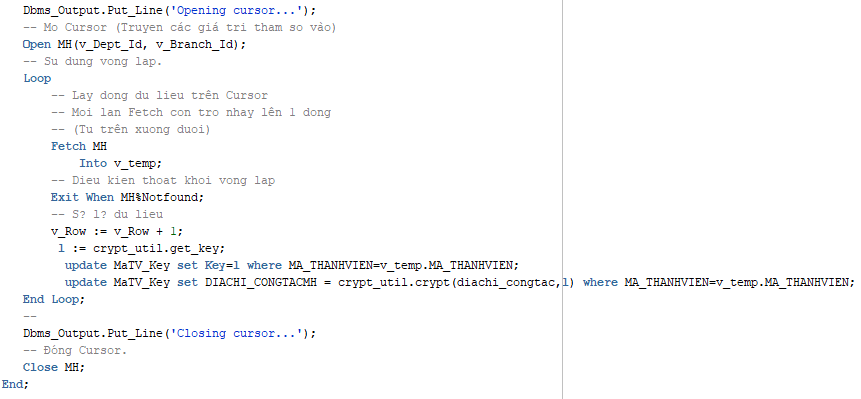


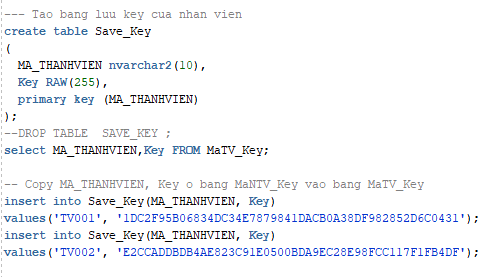


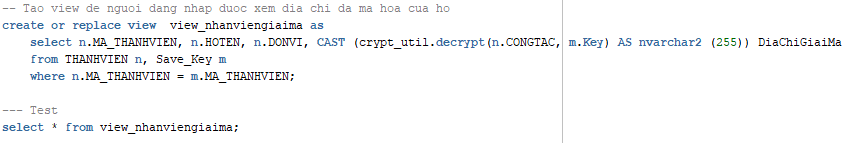














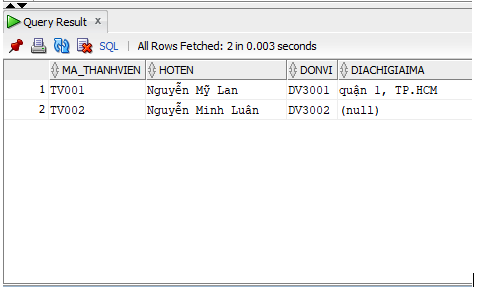


* Kết quả mã hóa:

A screenshot of a social media post

Description automatically generated

* Kết quả giải mã và phân quyền chỉ có TV001 mới được xem CONGTAC:



***Giao diện Mã hóa:***

***A screenshot of a cell phone

Description automatically generated***