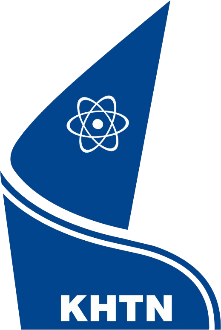


BÁO CÁO

ĐỒ ÁN

AN TOÀN VÀ BẢO MẬT

CƠ SỞ DỮ LIỆU

** **

TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN

KHOA CÔNG NGHỆ THÔNG TIN

1. **Thông tin nhóm.**

|  |  |  |  |
| --- | --- | --- | --- |
| Mã nhóm | MSSV | Họ tên | Email |
| **7** | **1412558** | **Phạm Quốc Toàn** | [**bossdiemmaimai@gmail.com**](mailto:bossdiemmaimai@gmail.com) |
| 1412657 | Nguyễn Tường Vy | [vytuong1120@gmail.com](mailto:vytuong1120@gmail.com) |
| 1412140 | Nguyễn Thị Thu Hà |  |

1. **Thông tin đồ án.**

Dựa vào mô tả quy trình quản lý tham gia đề án của một công ty để đưa ra lược đồ CSDL. Từ các yêu cầu bảo mật của dự án mà xác định cài đặt các cơ chế bảo mật như:

* Xác thực người dùng
* Điều khiển truy cập (DAC, RBAC, VPD, MAC)
* Mã hóa
* Auditing

Từ đó phân tích các cơ chế, chính sách sẽ dùng và cài đặt trên Hệ quản trị cơ sở dữ liệu Oracle.

1. **Hệ thống dành cho người quản trị bảo mật.**
2. **Các kiến thức cần có để thực hiện chức năng.**
   * Biết sử dụng một ngôn ngữ lập trình giao diện.
   * Cách kết nối đến Oracle Database.
   * Cách gọi và thực thi các câu lệnh R, I, U, D và các lệnh khác.
   * Cách tạo role/user, phân quyền cho role/user.
   * Biết khai thác một số System – Object và Table Data Dictionary cần thiết cho đồ án.
3. **Các chức năng đã làm.**

|  |  |  |
| --- | --- | --- |
| **STT** | **Tên chức năng** | **Ghi chú** |
| 1 | Nhận diện người quản trị và hiện giao diện tương ứng |  |
| 2 | Xem danh sách các đối tượng trên CSDL (Users, Tables, Roles) |  |
| 3 | Thêm mới đối tượng (User, Role) |  |
| 4 | Phân quyền, thu quyền của Role |  |
| 5 | Phân Role, thu Role của User |  |
| 6 | Xem các quyền của một User |  |

1. **Hiện thực các chính sách bảo mật.**
   1. **Lược đồ CSDL.**

**NHANVIEN** (**MANV**, HOTEN, PHAI, NGAYSINH, LUONG, PHUCAP, SODIENTHOẠI, PHONGBAN, CAPBAC).

**PHONGBAN** (**MAPHONG**, TENPHONG, NGAYNHANCHUC, TRUONGPHONG)

**DEAN** (**MADA**, TENDA, NGAYBD)

**THAMGIADEAN** (**MANV, MADA**, CHAMCONG, TRANGTHAI).

* 1. **Các ràng buộc, chú thích.**

Cấp bậc 1 là giám đốc, 2 là trưởng phòng, 3 là nhân viên thường

1. **Các chính sách, yêu cầu phân quyền.**
   1. **Các chính sách yêu cầu.**
      1. **Nhân viên nói chung được:**

Xem toàn bộ thông tin của chính bản thân mình.

Sữa dữ liệu của chính mình bao gồm (HOTENNV, NGAYSINH, SDT).

* + 1. **Nhân viên phòng nhân sự được:**

Xem chi tiết dữ liệu của các nhân viên, ngoại trừ trưởng phòng, giám đốc.

Sữa cột LUONG, PHUCAP, PHONGBAN của các nhân viên, ngoại trừ các nhân viên đó là trưởng phòng.

Xem chi tiết bảng tham gia đề án.

* + 1. **Nhân viên phòng kinh doanh được:**

Xem chi tiêt bảng đề án và bảng tham gia đề án.

* + 1. **Nhân viên phòng đề án được:**

Xem chi tiết bảng đề án và bảng tham gia đề án

Đăng ký hoặc hủy đăng ký tham gia đề án của chính họ.

* + 1. **Nhân viên phòng kế hoạch được:**

Xem, thêm, xóa, sữa bảng đề án.

* + 1. **Nhân viên làm trưởng phòng được:**

Xem chi tiết thông tin các nhân viên do mình quản lý.

Xem chi tiết bảng đề án và bảng tham gia đề án.

* + 1. **Nhân viên làm trưởng phòng đề án được:**

Cập nhật trạng thái tham gia đề án (cột TRANGTHAI).

Chấm công cho nhân viên tham gia đề án (cột CHAMCONG).

* + 1. **Nhân viên làm giám đốc được:**

Xem chi tiết thông tin các nhân viên.

Sữa lương, phụ cấp, phòng ban của các nhân viên thuộc cùng phòng với chính mình.

Xem chi tiết bản đề án và bảng đăng ký tham gia đề án.

* Tạo các role và gán các quyền tương ứng.
  1. **Ma trận truy vấn các bảng dữ liệu.**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **BẢNG NHÂN VIÊN** | | | | | | | | | |
|  | MANV | HOTEN | PHAI | NGAYSINH | SDT | LUONG | PHUCAP | PHONGBAN | CAPBAC | GHI CHÚ |
| Nhân viên | R | R, U | R, U | R, U | R, U | R | R | R | R | R, U dữ diệu chính mình |
| Nhân viên phòng nhân sự | R | R | R | R | R | R, U | R, U | R, U | R | Không được R, U của các trưởng phòng |
| Nhân viên làm trưởng các phòng | R | R | R | R | R | R | R | R | R | Chỉ được R các nhân viên thuộc phòng mình quản lý |
| Nhân viên làm giám đốc | R | R | R | R | R | R, U | R, U | R, U | R | R toàn bộ, chỉ được U các nhân viên thuộc cùng phòng với chính mình |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **BẢNG THAM GIA ĐỀ ÁN** | | | | | |
|  | MANV | MADEAN | THOIGIAN | TRANGTHAI | GHI CHÚ |
| Nhân viên phòng nhân sự | R | R | R | R | Xem chi tiết và đầy đủ bảng |
| Nhân viên phòng đề án | R, I, D | R, I, D | R, I, D | R, I, D | R, I, D chính họ |
| Nhân viên phòng kinh doanh | R | R | R | R | Xem chi tiết và đầy đủ bảng |
| Nhân viên làm trưởng các phòng | R | R | R | R | Xem chi tiết và đầy đủ bảng |
| Nhân viên làm trưởng phòng đề án | R | R | R, U | R, U | Xem chi tiết và đầy đủ bảng |
| Nhân viên làm giám đốc | R | R | R | R | Xem chi tiết và đầy đủ bảng |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **BẢNG ĐỀ ÁN** | | | | |
|  | MADE | TENDEAN | NGAYBD | GHI CHÚ |
|  |  |  |  |  |
| Nhân viên phòng đề án | R | R | R | Xem chi tiết và đầy đủ bảng |
| Nhân viên phòng kinh doanh | R | R | R | Xem chi tiết và đầy đủ bảng |
| Nhân viên phòng kế hoạch | R, I, U, D | R, I, U, D | R, I, U, D | RIUD toàn bộ bảng |
| Nhân viên làm trưởng phòng | R | R | R | Xem chi tiết và đầy đủ bảng |
| Nhân viên làm giám đốc | R | R | R |  |

1. **Kịch bản kiểm thử các chính sách bảo mật.**
   1. **DAC – RBAC – OLS**

* Dùng DAC cấp các quyền tương ứng cho các Role.
* Lấy các Role cấp cho người dùng là nhân viên.
  + 1. **Giám đốc có quyền xem toàn bộ bảng nhân viên.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **User** | **Role** | **Thao tác** | **Bảng** | **Kết quả** |
| **NV100** | **ROLE\_GIAMDOC** | **Select \* from NHANVIEN** | **NHANVIEN** | **Toàn bộ bảng nhân viên** |

* 1. **VPD**
* Xây dựng PACKAGE, các SYS\_CONTEXT để trả về vị từ.
* Cài đặt Trigger để tự tạo vị từ mỗi khi có user session đăng nhập.
* Đặt chính sách lên bảng dữ liệu
  + 1. **Nhân viên thông thường chỉ được xem thông tin của mình**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **User** | **Role** | **Thao tác** | **Bảng** | **Kết quả** |
| **NV107** | **ROLE\_NHANVIEN** | **Select \* from NHANVIEN** | **NHANVIEN** | **Dòng dữ liệu có MANV = NV107** |

* + 1. **Trưởng phòng được xem thông tin các nhân viên của chính mình.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **User** | **Role** | **Thao tác** | **Bảng** | **Kết quả** |
| **NV106** | **ROLE\_TRUONG**  **\_PHONG** | **Select \* from NHANVIEN** | **NHANVIEN** | **Các nhân viên thuộc phòng có MAPHONG = ‘PB002’ (mã phòng của NV106)** |
| **NV111** | **ROLE\_TRUONG**  **\_PHONG** | **Select \* from NHANVIEN** | **NHANVIEN** | **Các nhân viên thuộc phòng có MAPHONG = ‘PB003’ (mã phòng của NV111)** |

* 1. **OLS**
     1. **Nhân viên phòng nhân sự có quyền xem toàn bộ bảng nhân viên ngoại trừ thông tin trưởng phòng và giám đốc.**
* Tạo nhãn 1 mức (level).
* Cấp nhãn cho các tài khoản nhân viên.
* Thiết lập giá trị nhãn lên các dòng dữ liệu của bảng nhân viên.
* Đặt chính sách lên bảng dữ liệu

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **User** | **Role** | **Thao tác** | **Bảng** | **Kết quả** |
| **NV102** | **ROLE\_NV\_PHONG\_NHANSU** | **Select \* from NHANVIEN** | **NHANVIEN** | **Toàn bộ bảng nhân viên, trừ giám đốc, trưởng phòng** |

* 1. **Mã hóa**
* Mã hóa cột chấm công sao cho nhân viên tham gia đề án mới xem được dữ liệu của chính họ, không xem được của người khác
* Tạo Hash\_key cho bảng THAMGIADEAN từ key người dùng
* Mã hóa chấm công dùng key người dùng
* Giải mã dựa trên key người dùng nhập vào, kiểm tra hash
* Hiển thị view XEMCHAMCONG cho người dùng