**ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH**

**TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN**

**KHOA CÔNG NGHỆ THÔNG TIN**

\*\*\*



**BÁO CÁO ĐỒ ÁN**

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

**ỨNG DỤNG QUẢN LÝ THÔNG TIN   
VÀ CÔNG VIỆC CỦA NHÂN VIÊN**

**Giảng viên hướng dẫn:** **TS. Phạm Thị Bạch Huệ**

**ThS. Lê Vĩ Minh**

**ThS. Tiết Gia Hồng**

**Nhóm thực hiện: Nhóm 20H3T-16**

**Lớp: 20\_21**

*Thành phố Hồ Chí Minh, tháng 6/2023*

# MỤC LỤC

[MỤC LỤC 2](#_Toc139135245)

[MỤC LỤC HÌNH ẢNH 3](#_Toc139135246)

[1. TỔNG QUAN 5](#_Toc139135247)

[1.1. Thông tin chung 5](#_Toc139135248)

[1.2. Thông tin thành viên 5](#_Toc139135249)

[1.3. Đánh giá tham gia 5](#_Toc139135250)

[2. PHÂN CHIA CÔNG VIỆC 6](#_Toc139135251)

[2.1. Phân hệ 1 6](#_Toc139135252)

[2.2. Phân hệ 2 7](#_Toc139135253)

[3. ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH 8](#_Toc139135254)

[4. NỘI DUNG BÁO CÁO 9](#_Toc139135255)

[4.1. Thông tin đồ án 9](#_Toc139135256)

[4.2. Phân hệ 1: Hệ thống dành cho người quản trị bảo mật 9](#_Toc139135257)

[4.2.1. Màn hình đăng nhập 9](#_Toc139135258)

[4.2.2. Màn hình chính 10](#_Toc139135259)

[4.2.3. Màn hình chức năng xem danh sách người dùng hệ thống 11](#_Toc139135260)

[4.2.4. Màn hình cho chức năng xem bảng và view 12](#_Toc139135261)

[4.2.5. Màn hình cho phép thực hiện việc cấp quyền, thu hồi quyền, và xem quyền hiện có của người dùng 12](#_Toc139135262)

[4.2.6. Màn hình cho xem quyền hệ thống của người dùng 14](#_Toc139135263)

[4.2.7. Màn hình cho phép thêm, xóa, chỉnh sửa thông tin user/ role. 17](#_Toc139135264)

[4.3. Phân hệ 2: Hiện thực các chính sách bảo mật 18](#_Toc139135265)

[4.3.1. Tính năng hệ thống 18](#_Toc139135266)

[4.3.2. Lược đồ CSDL 29](#_Toc139135267)

[4.3.3. Các chính sách bảo mật 29](#_Toc139135268)

[4.3.4. Mã hóa 42](#_Toc139135269)

[4.3.5. Audit: 46](#_Toc139135270)

[5. HƯỚNG DẪN SỬ DỤNG 54](#_Toc139135271)

[6. TÀI LIỆU THAM KHẢO 54](#_Toc139135272)

# MỤC LỤC HÌNH ẢNH

[Hình 1. Giao diện đăng nhập 10](#_Toc139134405)

[Hình 2. Giao diện màn hình chính 10](#_Toc139134406)

[Hình 3. Giao diện xem danh sách người dùng 11](#_Toc139134407)

[Hình 4.Giao diện xem bảng và view trong cơ sở dữ liệu 12](#_Toc139134408)

[Hình 5. Giao diện thực hiện việc cấp quyền 13](#_Toc139134409)

[Hình 6. Giao diện cấp quyền Role cho User 14](#_Toc139134410)

[Hình 7. Màn hình kiểm tra quyền user 15](#_Toc139134411)

[Hình 8. Kết quả kiểm tra quyền user 15](#_Toc139134412)

[Hình 9. Giao diện kiểm tra quyền của Role 16](#_Toc139134413)

[Hình 10. Kết quả kiểm tra quyền Role 16](#_Toc139134414)

[Hình 11. Giao diện thao tác với User/Role 17](#_Toc139134415)

[Hình 12. Giao diện vai trò **Nhân viên** xem và sửa thông tin cá nhân 19](#_Toc139134416)

[Hình 13. Giao diện vai trò **Nhân viên** xem Phòng ban 19](#_Toc139134417)

[Hình 14. Giao diện vai trò **Nhân viên** xem bảng Đề Án 20](#_Toc139134418)

[Hình 15. Giao diện vai trò **Nhân viên** xem phân công của mình 20](#_Toc139134419)

[Hình 16. Giao diện vai trò Quản lý xem được nhân viên mình quản lý 21](#_Toc139134420)

[Hình 17. Giao diện vai trò **Quản lý** xem được phân công của mình và nhân viên mình quản lý 22](#_Toc139134421)

[Hình 18. Giao diện vai trò **Trưởng phòng** chỉ xem được nhân viên phòng ban mình quản lý 23](#_Toc139134422)

[Hình 19. Giao diện vai trò Trưởng phòng thêm, xóa, sửa phân công phòng ban mình quản lý 23](#_Toc139134423)

[Hình 20. Giao diện vai trò **Tài chính** xem được toàn bộ quan hệ **NHANVIEN** 24](#_Toc139134424)

[Hình 21. Giao diện vai trò **Tài chính** xem được toàn bộ quan hệ **PHANCONG** 25](#_Toc139134425)

[Hình 22. Giao diện vai trò **Tài chính** sửa lương của Nhân viên 25](#_Toc139134426)

[Hình 23. Giao diện vai trò Tài chính sửa phụ cấp của Nhân viên 26](#_Toc139134427)

[Hình 24. Giao diện vai trò **Nhân sự** thêm, cập nhật trên quan hệ **PHONGBAN** 27](#_Toc139134428)

[Hình 25. Giao diện vai trò **Nhân sự** thêm, cập nhật trên quan hệ **NHANVIEN** 27](#_Toc139134429)

[Hình 26. Giao diện vai trò **Trưởng đề án** thêm, xóa, sửa trên quan hệ **DEAN** 28](#_Toc139134430)

[Hình 27. Lược đồ cơ sở dữ liệu quan hệ được cài đặt 29](#_Toc139134431)

[Hình 28. Giao diện hiển thị các thông báo cho **một giám đốc có thể đọc được toàn bộ dữ liệu** 37](#_Toc139134432)

[Hình 29. Giao diện hiển thị các thông báo mà **Trưởng phòng sản xuất miền Nam** có quyền đọc 38](#_Toc139134433)

[Hình 30. Giao diện hiển thị các thông báo mà các **giám đốc ở miền Bắc** có quyền đọc 39](#_Toc139134434)

[Hình 31. Giao diện phán tán dòng thông báo t1 40](#_Toc139134435)

[Hình 32.Giao diện phát tán dòng thông báo t2 40](#_Toc139134436)

[Hình 33. Giao diện hiển thị các dòng thông báo mà Nhân viên sản xuất tại miền Nam có thể đọc 41](#_Toc139134437)

[Hình 34. Giao diện hiển thị dòng thông báo được phát tán cho toàn bộ Nhân viên. 42](#_Toc139134438)

[Hình 35. Giao diện chức năng Standard Audit 51](#_Toc139134439)

[Hình 36. Giao diện chức năng **Fine Gained Audit** 51](#_Toc139134440)

[Hình 37. Giao diện chức năng **Trigger Audit** 52](#_Toc139134441)

# TỔNG QUAN

## Thông tin chung

- Thông tin nhóm: Nhóm 20H3T-16

- Số lượng thành viên: 4 người

## Thông tin thành viên

|  |  |  |  |
| --- | --- | --- | --- |
| STT | MSSV | Họ và tên | Email |
| 1 | 20120255 | Phạm Mai Thiên Bảo | 20120255@student.hcmus.edu.vn |
| 2 | 20120295 | Ngô Võ Quang Huy | 20120295@student.hcmus.edu.vn |
| 3 | 20120305 | Võ Thị Kiều Khanh | 20120305@student.hcmus.edu.vn |
| 4 | 20120318 | Nguyễn Lê Mỹ Linh | 20120318@student.hcmus.edu.vn |

## Đánh giá tham gia

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Họ và tên | Mức độ  hoàn thành (%) | Mức độ  đóng góp (%) |
| 1 | Phạm Mai Thiên Bảo | 100 | 25 |
| 2 | Ngô Võ Quang Huy | 100 | 25 |
| 3 | Võ Thị Kiều Khanh | 100 | 25 |
| 4 | Nguyễn Lê Mỹ Linh | 100 | 25 |

# PHÂN CHIA CÔNG VIỆC

## Phân hệ 1

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung công việc | Phụ trách | Đánh giá của nhóm |
| 1 | * Tạo form cho phép tạo mới, xóa, sửa, user hoặc role. * Cho phép thu hồi quyền từ người dùng/ role. * Làm file hướng dẫn chạy | 20120255 | 10/10 |
| 2 | * Tạo form cho phép kiểm tra quyền của các chủ thể vừa dc cấp quyền * Tạo form cho phép chỉnh sửa quyền của user/role * Quay video demo | 20120295 | 10/10 |
| 3 | * Tạo form chức năng đăng nhập, trang chủ, cấp quyền cho user, cấp quyền cho role, cấp role cho user * Tạo giao diện quyền hiện có của 1 user/role * Phân chia công việc * Tổng hợp code | 20120305 | 10/10 |
| 4 | * Tạo form xem danh sách người dùng cho hệ thống * Tạo form xem thông tin về quyền (privileges) của mỗi user/ role trên các đối tượng dữ liệu. * Xem các bảng và view trong CSDL * Làm báo cáo phân hệ 1 | 20120318 | 10/10 |

## Phân hệ 2

|  |  |  |  |
| --- | --- | --- | --- |
| STT | Nội dung công việc | Phụ trách | Đánh giá của nhóm |
| 1 | * Thực hiện CS3 – Trưởng phòng * Thực hiện CS4 – Tài chính * Làm giao diện CS3 * Thực hiện OLS trên Oracle và demo * Thực hiện audit b và giao diện audit * Làm báo cáo các phần nêu trên | 20120255 | 10/10 |
| 2 | * Thực hiện CS6 – Trưởng đề án * Viết script khởi tạo database và thêm   dữ liệu mẫu.   * Làm giao diện CS4 * Thực hiện chính sách mã hóa dữ liệu và giải mã * Làm giao diện thay đổi mật khẩu * Thực hiện audit c và giao diện audit * Làm báo cáo các phần đã nêu trên | 20120295 | 10/10 |
| 3 | * Thực hiện CS5 – Nhân sự * Làm giao diện CS1 và CS5 * Làm giao diện xem Lương và Phụ cấp * Thực hiện chính sách mã hóa dữ liệu và giải mã * Thực hiện audit d * Tổng hợp file script chính sách * Tổng hợp và hoàn thiện báo cáo | 20120305 | 10/10 |
| 4 | * Thực hiện CS1 - Nhân viên * Thực hiện CS2 - QL trực tiếp * Làm giao diện CS2 và CS6 * Thực hiện audit a * Vẽ CSDL và đặc tả * Làm báo cáo các phần đã nêu trên | 20120318 | 10/10 |

# ĐÁNH GIÁ MỨC ĐỘ HOÀN THÀNH

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| STT | Yêu cầu | | Độ hoàn thành (%) | Hạn chế |
| 1 | Phân hệ 1 | Xem danh sách các đối tượng hiện có trên CSDL (user, role, table, view) | 100 | 0 |
| Thêm mới đối tương (table, user, role) | 100 | 0 |
| Phân quyền/Lấy lại quyền của 1 user/role | 100 | 0 |
| Xem quyền của 1 chủ thể | 100 | 0 |
| 2 | Phân hệ 2 | Lược đồ CSDL cuối cùng cài đặt | 100 | 0 |
| Liệt kê các chính sách bảo mật, phân tích và phân loại, đề ra giải pháp và cài đặt | 100 | 0 |
| Hoàn thiện cài đặt các chính sách bảo mật nêu trong đồ án, gồm cài đặt mức cơ sở dữ liệu và cung cấp giao diện minh họa cho từng vai trò người dùng (DAC, RBAC, VPD, MAC). | 100 | 0 |
| Mã hóa (chỉ cần cài đặt 1 chính sách, trình bày rõ PP quản lý khóa, trao đổi khóa, thay đổi khóa) và giao diện. | 100 | 0 |
| Audit cơ bản và FGA (4 chính sách). | 100 | 0 |

# NỘI DUNG BÁO CÁO

## Thông tin đồ án

Đồ án được chia làm 2 phân hệ với những yêu cầu như sau:

- ***Phân hệ 1:*** Hệ thống dành cho người quản trị bảo mật. Sinh viên hãy xây dựng ứng dụng cho phép các người dùng có quyền quản trị thực hiện công việc.

- ***Phân hệ 2:*** Hiện thực các chính sách bảo mật. 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.

Sinh viên cần mô tả thông tin chặt chẽ, xây dựng ứng dụng Winform theo mô hình Client-Server để phục vụ cho nhu cầu tra cứu và quản lý thông tin trong hệ thống.

Trong bài báo cáo này, nhóm sẽ trình bày về ...

- Ngôn ngữ lập trình:

+ *Về back-end*: Cơ sở dữ liệu Oracle.

+ *Về Front-end*: Winform C#.

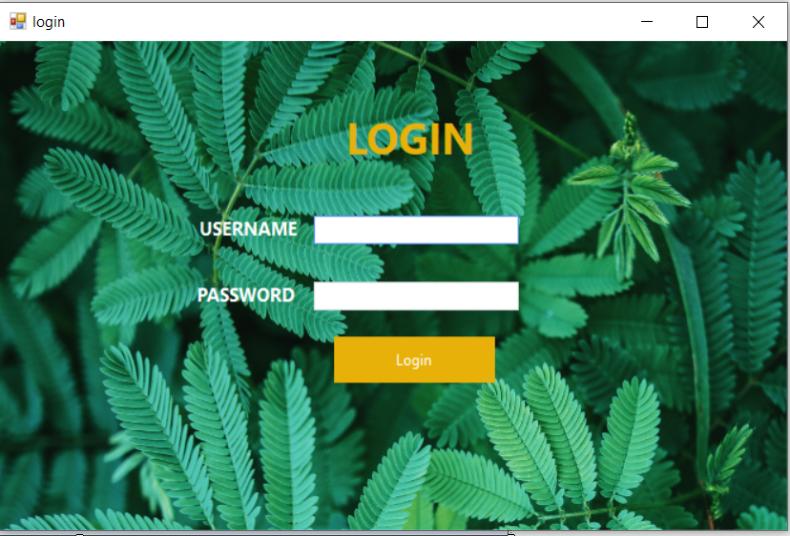
## Phân hệ 1: Hệ thống dành cho người quản trị bảo mật

### Màn hình đăng nhập

- Với màn hình giao diện đăng nhập, người dùng cần điền chính xác thông tin tài khoản được cấp cho bản thân. Từ đó, tùy theo vai trò người dùng trong hệ thống mà màn hình sẽ chuyển sang giao diện thích hợp cho người dùng đó.

- Cụ thể, trong phân hệ 1 này, người dùng cần có vai trò là DBA trong hệ thống thì mới có thể vào được giao diện dành cho người quản trị bảo mật.

- Và nếu người dùng nhập sai tài khoản, màn hình sẽ xuất thông báo lỗi cho người dùng biết.



Hình . Giao diện đăng nhập

### Màn hình chính

A screenshot of a computer

Description automatically generated with low confidence

Hình . Giao diện màn hình chính

Giao diện này thể hiện các chức năng mà người quản trị bảo mật có thể sử dụng để quản lý hệ thống. Tùy vào chức năng mà người quản trị chọn, màn hình sẽ xuất hiện giao diện chức năng đó thể người quản trị có thể thao tác.

### Màn hình chức năng xem danh sách người dùng hệ thống

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Giao diện xem danh sách người dùng

Giao diện này giúp quản trị viên quản lý được các người dùng có trong cơ sở dữ liệu. Thông tin sẽ được sắp xếp giảm dần theo ngày tạo.

### Màn hình cho chức năng xem bảng và view

A screenshot of a computer

Description automatically generated

Hình .Giao diện xem bảng và view trong cơ sở dữ liệu

Giao diện này giúp quản trị viên quản lý được các **table và view** có trong cơ sở dữ liệu.

### Màn hình cho phép thực hiện việc cấp quyền, thu hồi quyền, và xem quyền hiện có của người dùng

- Việc cấp quyền cho người dùng khi nhấn vào chức năng **“GRANT/REVOKE ROLE/USER”**.

- Với giao diện này, người dùng có thể thực hiện các chức năng như: cấp quyền cho user, cấp quyền cho role, thu hồi quyền cho user, cấp quyền từ role này cho user khác. 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 tính đến mức cột; quyền insert, delete thì không.

A screenshot of a computer screen

Description automatically generated with low confidence

Hình . Giao diện thực hiện việc cấp quyền

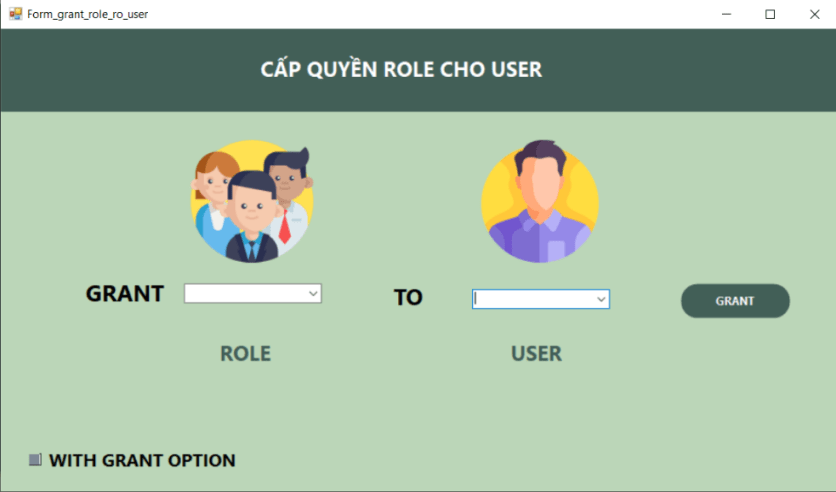
- Trong Role có danh sách các vai trò mà chính DBA đăng nhập vô hệ thống tạo ra.

- Trong User có danh sách các user do chính DBA đăng nhập vô hệ thống tạo ra.

- Chọn **Role** hoặc **User** cần để cấp quyền. Nhấn button “**CHECK\_USER**” để kiểm tra quyền của của user và nhấn button “**CHECK\_ROLE”** để kiểm tra quyền của role. Các quyền hiện có của Role hoặc user đó sẽ hiện lên trên bảng, từ đó người dùng có thể dựa vào đó để phân quyền.

- Nếu là user thì DBA có quyền chọn tất cả các ô check box có trên màn hình giao diện, DBA cũng có thể thu hồi quyền bằng cách bỏ chọn và nhấn “**SUBMIT\_USER**” để thực hiện việc cấp quyền hay thu hồi quyền.

Nếu là role thì các ô check box “**WITH GRANT OPTION**” vẫn có thể chọn nhưng khi nhấn “**SUBMIT\_ROLE**” thì các quyền với “**WITH GRANT OPTION**”.



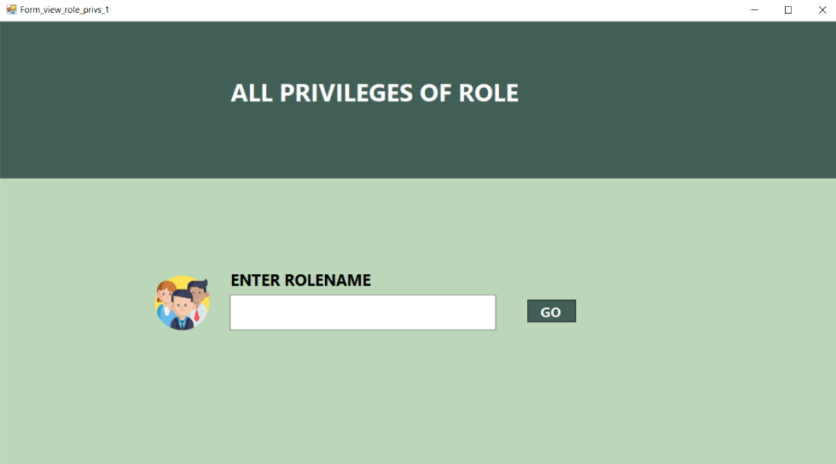
Hình . Giao diện cấp quyền Role cho User

- Việc cấp role cho user sẽ được tiến hành khi người dùng chọn **Role** và **User** ở 2 combobox, sau đó nếu muốn thì grant quyền theo “**WITH GRANT OPTION”**. Nhấn “**GRANT**” để hoàn thành việc cấp quyền cho role cho user.

### Màn hình cho xem quyền hệ thống của người dùng

Việc cho phép quản trị viên xem quyền của các chủ thể sẽ giúp cho quản trị viên có thể quản lí được các quyền của từng người dùng trong cơ sở dữ liệu, từ đó có thể đưa ra quyết định cấp quyền cần thiết cho người dùng hoặc có thể thu hồi lại các quyền dư thừa và không hợp lí từ người dùng. Điều này sẽ giúp cho cơ sở dữ liệu sẽ được an toàn hơn.

#### Kiểm tra quyền của user



Hình . Màn hình kiểm tra quyền user

Màn hình hiển thị yêu cầu quản trị viên điền username cần kiểm tra

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Kết quả kiểm tra quyền user

Sau khi nhập đúng username, hệ thống sẽ trả ra kết quả là bảng ‘**SYSTEM PRIVILEGES**’ tương ứng với quyền hệ thống trên các đối tượng trong cơ sở dữ liệu.

#### Kiểm tra quyền của role

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Giao diện kiểm tra quyền của Role

- Màn hình yêu cầu quản trị viên điền rolename cần tra cứu.

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Kết quả kiểm tra quyền Role

- Sau khi điền rolename chính xác, hệ thống sẽ trả ra kết quả là hai bảng ‘**SYSTEM PRIVILEGES**’ tương ứng với quyền hệ thống trên các đối tượng trong cơ sở dữ liệu.

### Màn hình cho phép thêm, xóa, chỉnh sửa thông tin user/ role.

- Giao diện cung cấp các thông tin về **User** và **Role** đã được tạo trong cơ sở dữ liệu, cho phép người dùng tạo (**CREATE**) một **User** hoặc **Role** mới; xóa (**DROP**), thay đổi (**ALTER**) mật khẩu cho **User** hoặc **Role** đã được tạo trước đó.

A screenshot of a computer

Description automatically generated

Hình . Giao diện thao tác với User/Role

- Để tạo một **User/Role** mới, người dùng cần nhập đầy đủ thông tin bao gồm tên **User/Role** và mật khẩu cho User/Role đó vào các **textbox Name** và **Password**. Sau đó người dùng click vào **button “Tạo User”** để tạo **User** mới hoặc **button “Tạo Role** để” tạo **Role** mới.

- Để xóa một **User/Role** đã tồn tại, người dùng cần nhập tên của **User/Role** cần xóa vào **textbox Name** và click vào **button “Xóa User”** để xóa **User** hoặc **button “Xóa Role”** để xóa **Role** đã tồn tại trong cơ sở dữ liệu.

- Để thay đổi thông tin (mật khẩu) của **User/Role** đã tồn tại trước đó, người dùng cần nhập đầy đủ thông tin bao gồm tên **User/Role** đã được tạo trước đó và mật khẩu mới cho **User/Role** đó vào các **textbox Name** và **Password**. Sau đó người dùng click vào **button “Đổi password User”** hoặc **button “Đổi password Role”** để thực hiện thay đổi mật khẩu của **User** hoặc **Role** tương ứng.

## Phân hệ 2: Hiện thực các chính sách bảo mật

### Tính năng hệ thống

#### Vai trò “**Nhân viên**”

Khi người dùng đăng nhập vào hệ thống có vai trò **Nhân viên** (**NV**), người dùng đó sẽ được:

- Xem thông tin cá nhân của bản thân và được sửa các thông tin *Ngày sinh, Địa chỉ, Số điện thoại* của bản thân (Không xem được của người khác đảm bảo tính bảo mật).

- Xem thông tin công việc được phân công của bản thân.

- Xem được danh sách các phòng ban trong công ty và các đề án mà công ty đang thực hiện.

**- Giao diện**

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

Hình . Giao diện vai trò **Nhân viên** xem và sửa thông tin cá nhân

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

Hình . Giao diện vai trò **Nhân viên** xem Phòng ban

Ảnh có chứa văn bản, ảnh chụp màn hình, số, phần mềm

Mô tả được tạo tự động

Hình . Giao diện vai trò **Nhân viên** xem bảng Đề Án

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

Hình . Giao diện vai trò **Nhân viên** xem phân công của mình

#### Vai trò “**Quản lý trực tiếp**”

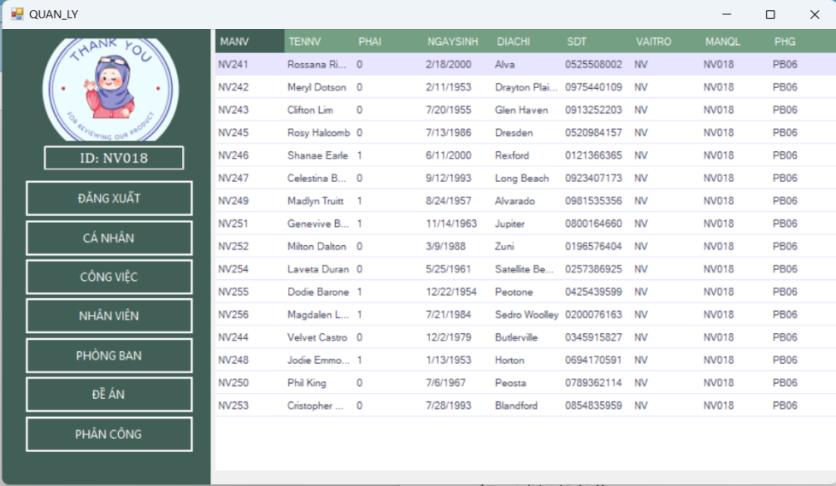
Khi người dùng đăng nhập vào hệ thống có vai trò **Quản lý trực tiếp** (**QL**), người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.

- Xem được thông tin các nhân viên mà mình quản lý (trừ thông tin *Lương, Phụ cấp* của nhân viên đó).

- Xem được thông tin phân công công việc của những nhân viên mà mình quản lý.

**- Giao diện**



Hình . Giao diện vai trò Quản lý xem được nhân viên mình quản lý

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

Hình . Giao diện vai trò **Quản lý** xem được phân công của mình và nhân viên mình quản lý

#### Vai trò “**Trưởng phòng**”

Khi người dùng đăng nhập vào hệ thống có vai trò **Trưởng phòng** (**TP**), người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.

- Xem được thông tin các nhân viên thuộc phòng ban mình quản lý (trừ thông tin *Lương, Phụ cấp* của nhân viên đó).

- Quản lý thông tin phân công công việc (thêm, xóa, cập nhật) của những nhân viên thuộc phòng ban mình quản lý.

**- Giao diện**

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Phông chữ

Mô tả được tạo tự động

Hình . Giao diện vai trò **Trưởng phòng** chỉ xem được nhân viên phòng ban mình quản lý

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

Hình . Giao diện vai trò Trưởng phòng thêm, xóa, sửa phân công phòng ban mình quản lý

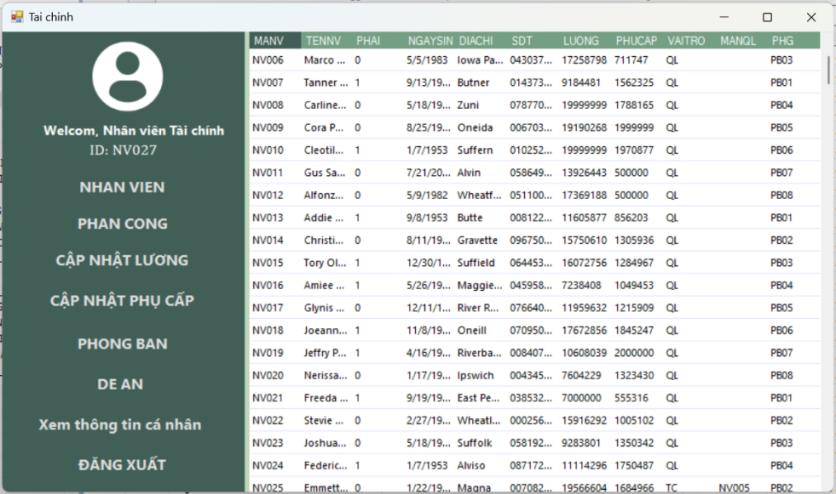
#### Vai trò “**Tài chính**”

Khi người dùng đăng nhập vào hệ thống có vai trò **Tài chính** (**TC**), người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.

- Xem được toàn bộ thông tin tất cả nhân viên trong công ty (thừa hành ban giám đốc) và được sửa thông tin *Lương, Phụ cấp* của một nhân viên bất kỳ.

**- Giao diện**



Hình . Giao diện vai trò **Tài chính** xem được toàn bộ quan hệ **NHANVIEN**

Ảnh có chứa văn bản, ảnh chụp màn hình, số, Phông chữ

Mô tả được tạo tự động

Hình . Giao diện vai trò **Tài chính** xem được toàn bộ quan hệ **PHANCONG**

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Biểu tượng máy tính

Mô tả được tạo tự động

Hình . Giao diện vai trò **Tài chính** sửa lương của Nhân viên

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

Hình . Giao diện vai trò Tài chính sửa phụ cấp của Nhân viên

#### Vai trò “**Nhân sự**”

Khi người dùng đăng nhập vào hệ thống có vai trò **Nhân sự** (**NS**), người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.

- Quản lý thông tin phòng ban của công ty (Thêm, sửa).

- Quản lý thông tin nhân viên trong công ty (Thêm, sửa nhưng trừ thông tin *Lương, Phụ cấp* của nhân viên và cũng không được xem hai thông tin này).

- Giao diện

Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, số

Mô tả được tạo tự động

Hình . Giao diện vai trò **Nhân sự** thêm, cập nhật trên quan hệ **PHONGBAN**

Ảnh có chứa văn bản, ảnh chụp màn hình, số, phần mềm

Mô tả được tạo tự động

Hình . Giao diện vai trò **Nhân sự** thêm, cập nhật trên quan hệ **NHANVIEN**

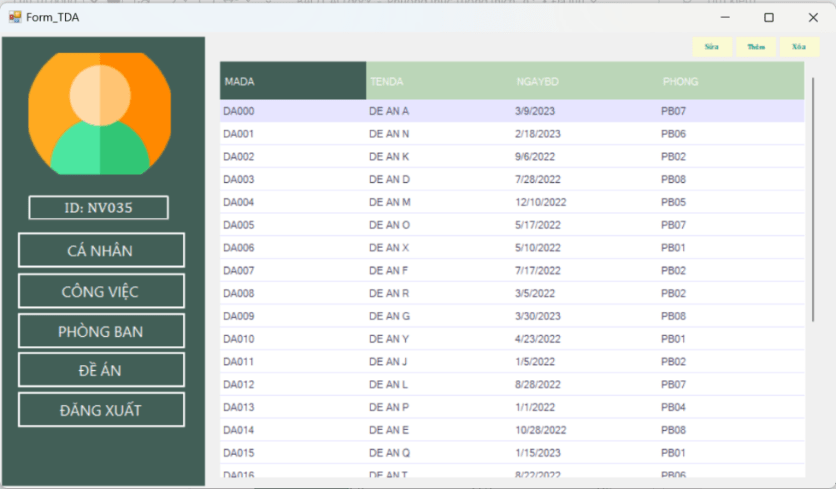
#### Vai trò “**Trưởng đề án**”

Khi người dùng đăng nhập vào hệ thống có vai trò **Trưởng đề án** (**TDA**), người dùng đó sẽ được:

- Có các tính năng của vai trò *Nhân viên*.

- Quản lý thông tin đề án của công ty (Thêm, xóa, sửa).

- **Giao diện**



Hình . Giao diện vai trò **Trưởng đề án** thêm, xóa, sửa trên quan hệ **DEAN**

#### Vai trò “**Ban giám đốc**”

Khi người dùng đăng nhập vào hệ thống có vai trò **Ban giám đốc** (**BGD**), người dùng đó sẽ được: Xem tất cả thông tin trong hệ thống nhưng không được thêm, xóa, sửa bất kỳ thông tin nào.

### Lược đồ CSDL

Ảnh có chứa văn bản, ảnh chụp màn hình, biểu đồ, hàng

Mô tả được tạo tự động

Hình . Lược đồ cơ sở dữ liệu quan hệ được cài đặt

### Các chính sách bảo mật

#### Chính sách DAC

- **DAC** là viết tắt của "**Discretionary Access Control**" (*Kiểm soát truy cập tùy ý*). Trong Oracle Database, DAC đề cập đến hệ thống kiểm soát truy cập dựa trên quyền hạn được xác định bởi người quản trị cơ sở dữ liệu hoặc chủ sở hữu đối tượng. DAC cho phép người quản trị hoặc chủ sở hữu quyết định và kiểm soát quyền truy cập tới các đối tượng cơ sở dữ liệu, chẳng hạn như bảng, chế độ xem, thủ tục lưu trữ và tài khoản người dùng.

- Trong hệ thống DAC của Oracle, người quản trị hoặc chủ sở hữu có thể gán các quyền cụ thể cho người dùng hoặc vai trò. Quyền hạn này có thể bao gồm quyền SELECT, INSERT, UPDATE, DELETE, EXECUTE và nhiều quyền khác. Người dùng hoặc vai trò chỉ có thể thực hiện các hoạt động trên đối tượng nếu được cấp phép.

- Ở phân hệ 2, mỗi người dùng sẽ được cấp một username riêng và mật khẩu riêng để đăng nhập vào cơ sở dữ liệu. Với nhiều số lượng người dùng nhiều hơn 100 người nên nhóm chúng em đã sử dụng phần lớn là RBAC thay cho DAC.

#### Chính sách RBAC

- **RBAC** là viết tắt của "**Role-Based Access Control**" (*Kiểm soát truy cập dựa trên vai trò*). RBAC là một phương pháp quản lý truy cập trong lĩnh vực an ninh thông tin, trong đó quyền hạn truy cập được gán dựa trên vai trò của người dùng.

- Trong hệ thống RBAC, người dùng được gán vào các vai trò khác nhau. Mỗi vai trò sẽ có một tập hợp các quyền hạn tương ứng với các hoạt động mà người dùng trong vai trò đó có thể thực hiện. Thay vì gán quyền truy cập cho từng người dùng cụ thể, quyền hạn được gán cho các vai trò và người dùng được gán vào các vai trò đó.

- Chương trình đã cài đặt chính sách này với từng trường hợp cụ thể, như sau:

* Đối với vai trò ‘**Nhân viên**’, chương trình cài đặt các view để kiểm soát người dùng chỉ được xem thông tin chính mình trong hai bảng **NHANVIEN** và **PHANCONG**. Và chỉ được cập nhật thông tin ngày sinh, địa chỉ và số điện thoại của mình trong bảng **NHANVIEN**.
* Đối với vai trò ‘**Quản lí**’, chương trình cài đặt cái view để người dùng chỉ được phép xem các thuộc tính ngoại trừ **LUONG** và **PHUCAP** của các nhân viên khác.
* Đối với vai trò ‘**Trưởng phòng**’, chương trình cài đặt view để người dùng chỉ *thêm, xoá, cập nhật* trên quan hệ **PHANCONG** của các nhân viên thuộc phòng ban của trưởng phòng đó.
* Đối với vai trò ‘**Tài chính**’, chương trình đã gán quyền xem trên bảng **PHANCONG** và **NHANVIEN**, ngoài ra người dùng còn được gán quyền cập nhật trên hai trường **LUONG** và **PHUCAP** trong quan hệ **NHANVIEN**.
* Đối với vai trò ‘**Nhân sự**’, chương trình đã gán quyền thêm, cập nhật trên quan hệ **PHONGBAN**.
* Đối với vai trò ‘**Trưởng đề án**’, chương trình đã gán quyền thêm, xóa, cập nhật trên quan hệ **DEAN**.

#### Chính sách VPD

- **VPD** là viết tắt của ‘**Virtual Private Database**’. VPD là một tính năng trong cơ sở dữ liệu Oracle cho phép triển khai các quy tắc bảo mật dữ liệu trên cơ sở dữ liệu mà không cần thay đổi ứng dụng hoặc schema hiện có. VPD cho phép kiểm soát quyền truy cập dựa trên các điều kiện động, dựa trên dữ liệu trong cơ sở dữ liệu và thông tin người dùng.

- VPD sử dụng các chức năng quyền (policy function) để xác định các quy tắc truy cập cho dữ liệu. Khi người dùng truy cập vào bất kỳ đối tượng nào trong cơ sở dữ liệu, VPD sẽ kích hoạt các chức năng quyền để xác định quyền truy cập của người dùng dựa trên các quy tắc được xác định trước.

- Chương trình đã cài đặt chính sách này với từng trường hợp cụ thể, như sau:

• Đối với vai trò ‘**Quản lí**’, chương trình đã cài đặt VPD để kiểm soát chỉ cho phép người dùng chỉ được xem thông tin của nhân viên do mình quản lí ngoại trừ hai trường **LUONG** và **PHUCAP**.

• Đối với vai trò ‘**Trưởng phòng**’, chương trình đã cài đặt vpd để giới hạn người dùng chỉ được phép xem các thông tin ngoại trừ **LUONG** và **PHUCAP** của nhân viên thuộc phòng ban của mình.

#### OLS:

##### Gán nhãn cho Giám đốc, Trưởng phòng và Giám đốc miền Bắc

**• Tạo Level:**

|  |  |  |  |
| --- | --- | --- | --- |
| **POLICY\_NAME** | **LONG\_NAME** | **SHORT\_NAME** | **LEVEL\_NUM** |
| ESBD | GIAM DOC | GD | 9000 |
| ESBD | TRUONG PHONG | TP | 8000 |
| ESBD | NHAN VIEN | NV | 7000 |

**• Tạo Compartment:**

|  |  |  |  |
| --- | --- | --- | --- |
| **POLICY\_NAME** | **LONG\_NAME** | **SHORT\_NAME** | **COMP\_NUM** |
| ESBD | MUA BAN | MB | 100 |
| ESBD | SAN XUAT | SX | 200 |
| ESBD | GIA CONG | GC | 300 |

**• Tạo Group:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **POLICY\_NAME** | **LONG\_NAME** | **SHORT\_NAME** | **GROUP\_NUM** | **PARRENT\_NAME** |
| ESBD | TAP DOAN S | S | 1 | NULL |
| ESBD | MIEN BAC | B | 10 | 1 |
| ESBD | MIEN TRUNG | T | 20 | 1 |
| ESBD | MIEN NAM | N | 30 | 1 |

**• Tạo Nhãn:**

Quy ước tạo nhãn để dễ dàng quản lý:

* Cấu trúc nhãn: xyzt
  + x: giá trị level quy ước.
  + y: giá trị compartment quy ước.
  + z: giá trị group quy ước.
  + t: giá trị dự phòng, mặc định t = 0.
* Level:
  + GD: 3
  + TP: 2
  + NV: 1
* Compartment:
  + SX: 1
  + GC: 2
  + MB: 3
  + Các nhãn bao gồm nhiều compartment thì lấy tổng các compartment thành phần làm giá trị quy ước.
* Group:
  + B: 1
  + T: 2
  + N: 3
  + Các nhãn bao gồm nhiều group thì lấy tổng các group thành phần làm giá trị quy ước.

|  |  |  |
| --- | --- | --- |
| **POLICY\_NAME** | **LABEL\_TAG** | **LABEL\_VALUE** |
| ESBD | GD | 3000 |
| ESBD | TP | 2000 |
| ESBD | NV | 1000 |
| ESBD | GD:MB,SX,GC:B,T,N | 3660 |
| ESBD | NV:SX:N | 1130 |
| ESBD | NV:MB,SX,GC:B,T,N | 1660 |
| ESBD | TP:SX:N | 2130 |
| ESBD | TP:SX:T | 2120 |
| ESBD | GD:SX,GC,MB:B | 3610 |
| ESBD | TP: MB,SX,GC:B,T,N | 2660 |
| ESBD | GD:GC:N | 3230 |

**• Gán nhãn cho một số người dùng:**

|  |  |  |  |
| --- | --- | --- | --- |
| **MÔ TẢ NGƯỜI DÙNG** | **POLICY\_NAME** | **USER\_NAME** | **MAX\_READ\_LABEL** |
| *Giám đốc quản lý toàn bộ công ty* | ESBD | GIAMDOC | GD: MB,SX,GC:B,T,N |
| *Giám đốc phụ trách tất cả các lĩnh vực ở miền Bắc* | ESBD | GIAMDOCMB | GD:MB,SX,GC:B |
| Trưởng phòng quản lý tất cả các chi nhánh. | ESBD | TRUONGPHONG | TP: MB,SX,GC:B,T,N |
| *Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Nam* | ESBD | TPSXMN | TP:SX:N |
| Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung | ESBD | TPSXMT | TP:SX:T |
| Nhân viên bình thường, không làm trong bất kì các lĩnh vực nào. | ESBD | NHANVIEN | NV |
| Giám đốc phụ trách lĩnh vực gia công ở miền Nam | ESBD | GIAMDOC\_GC\_MN | GD:GC:N |

##### Cách thức phát tán dòng thông báo t1 đến tất cả các Trưởng phòng không phân biệt lĩnh vực

❖ **REMOVE** chính sách OLS hiện tại (**ESBD**) trên bảng **ANNOUNCEMENTS**.

❖ Áp dụng lại chính sách **‘ESBD’** lên bảng **ANNOUNCEMENTS** với **TABLE\_OPTIONS => ‘NO\_CONTROL’**.

❖ Thêm dòng dữ liệu (thông báo t1) vào bảng **ANNOUNCEMENTS**.

❖ Thiết lập giá trị ROW\_LABEL của dòng dữ liệu bằng cách sử dụng phương thức: **CHAR\_TO\_LABEL (‘ESBD’, ‘TP’)**.

❖ Áp dụng lại chính sách **‘ESBD’** lên bảng **ANNOUNCEMENTS** một lần nữa với **TABLE\_OPTIONS => ‘READ\_CONTROL, CHECK\_CONTROL’**.

##### Cách thức phát tán dòng thông báo t2 đến tất cả các Trưởng phòng sản xuất miền Trung

❖ **REMOVE** chính sách OLS hiện tại (**ESBD**) trên bảng **ANNOUNCEMENTS**.

❖ Áp dụng lại chính sách **‘ESBD’** lên bảng **ANNOUNCEMENTS** với **TABLE\_OPTIONS => ‘NO\_CONTROL’**.

❖ Thêm dòng dữ liệu (thông báo t2) vào bảng **ANNOUNCEMENTS**.

❖ Thiết lập giá trị **ROW\_LABEL** của dòng dữ liệu bằng cách sử dụng phương thức: **CHAR\_TO\_LABEL (‘ESBD’, ‘TP:SX:T’)**.

❖ Áp dụng lại chính sách **‘ESBD’** lên bảng **ANNOUNCEMENTS** một lần nữa với **TABLE\_OPTIONS => ‘READ\_CONTROL, CHECK\_CONTROL’**.

##### Một số cách thức phát tán dòng dữ liệu khác

###### Phát tán dòng thông báo đến tất cả các nhân viên không phân biệt lĩnh vực, vị trí:

❖ **REMOVE** chính sách OLS hiện tại (**ESBD**) trên bảng **ANNOUNCEMENTS**.

❖ Áp dụng lại chính sách **‘ESBD’** lên bảng **ANNOUNCEMENTS** với **TABLE\_OPTIONS => ‘NO\_CONTROL’**.

❖ Thêm dòng dữ liệu vào bảng **ANNOUNCEMENTS**.

❖ Thiết lập giá trị **ROW\_LABEL** của dòng dữ liệu bằng cách sử dụng phương thức: **CHAR\_TO\_LABEL (‘ESBD’, ‘NV’)**.

❖ Áp dụng lại chính sách **‘ESBD’** lên bảng **ANNOUNCEMENTS** một lần nữa với **TABLE\_OPTIONS => ‘READ\_CONTROL, CHECK\_CONTROL’**.

###### Phát tán dòng thông báo đến các giám đốc gia công miền Nam

❖ **REMOVE** chính sách OLS hiện tại (**ESBD**) trên bảng **ANNOUNCEMENTS**.

❖ Áp dụng lại chính sách **‘ESBD’** lên bảng **ANNOUNCEMENTS** với **TABLE\_OPTIONS => ‘NO\_CONTROL’**.

❖ Thêm dòng dữ liệu vào bảng **ANNOUNCEMENTS**.

❖ Thiết lập giá trị **ROW\_LABEL** của dòng dữ liệu bằng cách sử dụng phương thức: **CHAR\_TO\_LABEL (‘ESBD’, ‘GD:GC:N’)**.

❖ Áp dụng lại chính sách ‘**ESBD’** lên bảng **ANNOUNCEMENTS** một lần nữa với **TABLE\_OPTIONS => ‘READ\_CONTROL. CHECK\_CONTROL’**.

##### Giao diện chức năng OLS

###### Một giám đốc có thể đọc được toàn bộ dữ liệu

Nhóm chúng em đã gán nhãn cho người dùng là “**NV000**” với nhãn là 'GD:MB,SX,GC:B,T,N' để cho người dùng này có vai trò giám đốc có thể đọc được toàn bộ thông báo.

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Giao diện hiển thị các thông báo cho **một giám đốc có thể đọc được toàn bộ dữ liệu**

###### Người dùng có vai trò trưởng phòng sản xuất Miền Nam

- Gán nhãn cho người dùng “**NV039**” với nhãn 'TP:SX:N' để cho người dùng này có vai trò Trưởng phòng sản xuất miền Nam.

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Giao diện hiển thị các thông báo mà **Trưởng phòng sản xuất miền Nam** có quyền đọc

###### Người dùng với vai trò giám đốc phụ trách bất kì lĩnh vực nào ở miền bắc

- Gán nhãn 'GD:MB,SX,GC:B' cho người dùng “**NV001**” để cho người dùng này trở thành Giám đốc miền Bắc.

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Giao diện hiển thị các thông báo mà các **giám đốc ở miền Bắc** có quyền đọc

###### Cách thức phát tán dòng thông báo t1 đến tất cả trưởng phòng phụ trách tất cả các lĩnh vực không phân biệt chi nhánh.

- Khi thêm vào bảng, thông báo t1 sẽ được gán nhãn ‘TP’ để cho các người dùng là trưởng phòng xem được thông báo này.

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Giao diện phán tán dòng thông báo t1

###### Cách thức phát tán dòng thông báo t2 đến trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung.

- Gán cho “NV042” và thông bào t2 cùng một nhãn ‘TP:SX:T’ để cho người dùng này trở thành Trưởng phòng phụ trách lĩnh vực sản xuất ở miền Trung và xem được thông báo t2.

A screenshot of a computer

Description automatically generated with medium confidence

Hình .Giao diện phát tán dòng thông báo t2

###### Một số kịch bản phụ

- Gán nhãn ‘NV:SX:N’ cho cho ‘NV047’, giả sử rằng đây là một Nhân viên sản xuất Miền Nam. Nhân viên này chỉ đọc được các thông báo gửi đến toàn bộ các nhân viên, các nhân viên sản xuất và các nhân viên có cùng nhãn với nhân viên này.

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Giao diện hiển thị các dòng thông báo mà Nhân viên sản xuất tại miền Nam có thể đọc

- Gán nhãn một thong báo với nhãn ‘NV’, đây sẽ là thông báo chứa thông tin có mức độ nhạy cảm thấp nhất, thông báo này sẽ được đọc bởi tất cả các người dùng được gán nhãn và cấp quyền truy cập vào bảng thông báo.

A screenshot of a computer

Description automatically generated with medium confidence

Hình . Giao diện hiển thị dòng thông báo được phát tán cho toàn bộ Nhân viên.

### Mã hóa

#### User vai trò gì thực hiện mã hóa?

User có vai trò là quản trị hệ thống hoặc quản trị cơ sở dữ liệu sẽ thực hiện mã hóa dữ liệu. Những người dùng này có quyền truy cập và sửa đổi cấu trúc dữ liệu và mã hóa.

#### Mã hóa dữ liệu ở mức nào?

Nhóm thực hiện mã hóa mức cơ sở dữ liệu (Database Level). Những lí do mà nhóm chọn mức mã hóa này:

* **Tính toàn vẹn của dữ liệu:** Mã hóa dữ liệu ở mức cơ sở dữ liệu đảm bảo tính toàn vẹn của dữ liệu. Dữ liệu được mã hóa trước khi lưu trữ, điều này đảm bảo rằng dữ liệu chỉ có thể được giải mã bởi những người có quyền truy cập.
* **Bảo mật toàn diện:** Mã hóa dữ liệu ở mức cơ sở dữ liệu bảo vệ thông tin nhạy cảm khỏi sự truy cập trái phép. Ngay cả khi dữ liệu bị lộ, thông tin sẽ không thể đọc được nếu không có khóa mã hóa phù hợp.
* **Tính linh hoạt:** Mã hóa dữ liệu ở mức cơ sở dữ liệu giúp đảm bảo tính riêng tư của thông tin mà không yêu cầu thay đổi cấu trúc lưu trữ dữ liệu. Các ứng dụng hoặc giao diện người dùng có thể tiếp tục hoạt động như bình thường, chỉ thay đổi ở mức cơ sở dữ liệu.
* **Chống được các kiểu tấn công:** đánh cắp thiết bị lưu trữ, tấn công mức cơ sở dữ liệu (ví dụ SQL injection), người quản trị truy cập dữ liệu bất hợp pháp
* Được đảm nhận thông qua việc dùng thủ tục hoặc trigger

Ở đây chúng em đã sử dụng cấp độ mã hóa cơ sở dữ liệu là ***Column/Atribute level (cấp độ cột/thuộc tính****)* cụ thể là mã hóa các thông tin trong cột **LUONG** và **PHUCAP**.

#### Có cần thay đổi gì về cấu trúc lưu trữ dữ liệu hay không?

Trong đề xuất giải pháp mã hóa dữ liệu ở mức cơ sở dữ liệu, không cần thay đổi cấu trúc lưu trữ dữ liệu. Dữ liệu vẫn được lưu trữ dưới dạng thông thường trong cơ sở dữ liệu, nhưng trước khi lưu trữ, thông tin liên quan đến trường LUONG và PHUCAP sẽ được mã hóa.

Việc mã hóa dữ liệu không yêu cầu thay đổi cấu trúc lưu trữ dữ liệu vì quá trình mã hóa và giải mã được thực hiện trên dữ liệu gốc trước khi lưu vào cơ sở dữ liệu. Khi cần truy xuất dữ liệu, quá trình giải mã sẽ được thực hiện để trả về dữ liệu ban đầu cho ứng dụng hoặc giao diện người dùng.

Điều này giúp bảo vệ tính riêng tư của thông tin nhân viên liên quan đến trường LUONG và PHUCAP mà không ảnh hưởng đến cấu trúc lưu trữ dữ liệu hiện có. Hệ thống và ứng dụng có thể tiếp tục hoạt động như bình thường mà không cần thay đổi cách lưu trữ dữ liệu.

#### Cơ chế quản lý khóa

Cơ chế mã hóa được áp dụng như sau:

❖ Thiết lập khoá

• Việc tạo khóa sẽ dựa trên mật khẩu người dùng.

• Nhóm chúng em đã sử dụng hàm **PBKDF2** (***Password-Based Key Derivation Function 2***) để tạo ra một khóa từ mật khẩu với muối.

• Với tham số đầu vào là mật khẩu ban đầu trong dạng VARCHAR2, muối, số lần lặp để gia tăng độ phức tạp thuật toán và một biến để yêu cầu độ dài khóa đầu ra mong muốn.

• Trong hàm có sử dụng thuật toán **HMAC-SHA1**(***HMAC-Secure Hash Algorithm 1***).

• Sau khi chạy hàm thì sẽ trả về kết quả cuối cùng, khóa đầu ra của hàm cũng với độ dài tương ứng bằng cách sử dựng hàm **UTL\_RAW.SUBSTR**.

• Mã hóa hai cột **LUONG** và **PHUCAP**

• Viết 1 thủ tục gọi là "**encrypt\_EACH\_NHANVIEN**" sử dụng 1 package mã hóa dữ liệu trên Oracle là **DBMS\_CRYPTO**. Trong package đó, nhóm em sử dụng một số phương pháp để hỗ trợ mã hóa dự liệu:

▪ **DBMS\_CRYPTO.ENCRYPT\_AES128**: Chọn thuật toán mã hóa AES với khóa 128 bit. Độ dài khóa 128-bit đảm bảo tính bảo mật cao đối với việc mã hóa dữ liệu. Việc sử dụng **DBMS\_CRYPTO.ENCRYPT\_AES128** trong thủ tục "**encrypt\_EACH\_NHANVIEN**" cho phép mã hóa dữ liệu lương và phụ cấp của nhân viên với một thuật toán mã hóa mạnh mẽ và bảo mật, đồng thời đảm bảo tính hiệu suất và tương thích với hệ thống Oracle Database.

▪ **DBMS\_CRYPTO.CHAIN\_CBC**: Chế độ **Cipher Block Chaining (CBC)** được sử dụng để mã hóa. Trong chế độ này, mỗi khối dữ liệu được mã hóa được kết hợp với khối trước đó trước khi tiến hành mã hóa.

▪ **DBMS\_CRYPTO.PAD\_PKCS5**: Chuẩn **PKCS5** được sử dụng để thực hiện padding cho dữ liệu. **Padding** là quá trình thêm các bytes đệm vào dữ liệu để đảm bảo độ dài của dữ liệu là bội số của kích thước khối mã hóa.

▪ **key**: Đây là khóa được sử dụng để mã hóa dữ liệu. Trong trường hợp này, khóa (v\_key) đã được tạo trước đó bằng cách sử dụng hàm **pbkdf2**.

▪ **iv**: Đây là vector khởi tạo (**Initialization Vector - IV**), được sử dụng trong quá trình mã hóa CBC. Trong trường hợp này, vector khởi tạo (**v\_iv**) đã được tạo ngẫu nhiên.

❖ Phân phối khoá

• Mỗi người dùng sau khi được tạo tài khoản thì sẽ được cấp mật khẩu ban đầu là username của mình và mật khẩu này cũng sẽ được dùng để làm khoá cho việc mã hoá hai trường ‘**LUONG**’ và ‘**PHUCAP**’.

• Sau khi đăng nhập lần đầu tiên, ứng dụng sẽ yêu cầu người dùng đổi mật khẩu trước khi sử dụng ứng dụng.

• Đối với chức năng ‘**Xem LUONG và PHUCAP**’ thì người dùng phải nhập đúng mật khẩu của mình mới được xem.

❖ Lưu trữ khoá

• Nhóm chúng em đã tạo ta một bảng **DANGNHAP** để *lưu trữ khóa tạo ra và vector khởi tạo iv*. Bằng cách lưu trữ khóa trên bảng đăng nhập, chúng em thể quản lý khóa một cách cụ thể cho từng người dùng và có thể áp dụng các chính sách bảo mật khác nhau cho khóa.

• Việc lưu trữ khóa trên bảng đăng nhập cũng có thể giúp quản lý và kiểm soát quyền truy cập vào khóa. Chỉ các người dùng được phép truy cập vào bảng đăng nhập mới có thể lấy được khóa. Điều này giúp đảm bảo rằng chỉ những người dùng có quyền truy cập hợp lệ mới có thể sử dụng khóa để giải mã dữ liệu.

* Phục hồi khóa

• **PBKDF2** được sử dụng để tạo khóa từ mật khẩu người dùng. Điều này đảm bảo rằng khóa mã hóa sẽ được tạo ra từ mật khẩu của người dùng một cách an toàn và không thể dễ dàng phục hồi. **PBKDF2** sử dụng một số lượng lặp lại và giá trị muối (salt) để tăng cường tính bảo mật. Quá trình tính toán **PBKDF2** là một hàm một chiều, nghĩa là không thể dễ dàng đảo ngược để phục hồi mật khẩu ban đầu từ khóa.

• Trong trường hợp người dùng quên mật khẩu của họ, không có cách trực tiếp để phục hồi khóa để giải mã cột Lương và Phụ Cấp. Thay vào đó, phương pháp phổ biến là yêu cầu người dùng tạo một mật khẩu mới và sử dụng nó để tạo khóa mới thông qua **PBKDF2**. Sau đó, bạn có thể sử dụng khóa mới này để giải mã và truy cập vào dữ liệu cột Lương và Phụ Cấp.

• Trong quá trình này, mật khẩu ban đầu sẽ không được phục hồi, và bạn sẽ cần thông báo cho người dùng về việc thay đổi mật khẩu và cập nhật dữ liệu mật khẩu mới. Điều này đảm bảo tính bảo mật và không cho phép ai khác truy cập vào dữ liệu bằng mật khẩu đã quên.

⇨ Tóm lại, trong trường hợp sử dụng PBKDF2 để tạo khóa AES-128 từ mật khẩu người dùng, việc phục hồi khóa khi người dùng quên mật khẩu không khả thi. Thay vào đó, việc thay đổi mật khẩu và tạo khóa mới thông qua PBKDF2 là cách tiếp cận thông thường.

❖ Thay đổi khoá

* Ứng dụng sẽ bắt buộc người dùng đăng nhập đầu tiên đổi mật khẩu trước khi tiếp tục sử dụng ứng dụng.
* Sau khi mật khẩu được đổi, mật khẩu sẽ được mã hoá bằng hàm **PBKDF2** và cập nhật lại trên quan hệ **DANGNHAP**.
* Tiếp theo, hai cột **LUONG** và **PHUCAP** trên quan hệ **NHANVIEN** của người dùng đó sẽ được mã hoá bằng mật khẩu mới và cập nhật lại trên quan hệ **NHANVIEN**.

### Audit:

#### Những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG.

❖ Phương thức sử dụng: FGA Audit.

❖ Cách thức cụ thể:

• Sử dụng gói **DBMS\_FGA**.

• Gọi thủ tục **ADD\_POLICY** và truyền các tham số để áp dụng chính sách audit lên bảng **PHANCONG** theo yêu cầu:

|  |  |
| --- | --- |
| **OBJECT\_SCHEMA** | COMPANY |
| **OBJECT\_NAME** | PHANCONG |
| **POLICY\_NAME** | A\_AUDIT |
| **AUDIT\_COLUMN** | THOIGIAN |
| **STATEMENT\_TYPES** | UPDATE |
| **ENABLE** | TRUE |

⇨ Chính sách sẽ ghi lại các hoạt động **UPDATE** trên cột **THOIGIAN** của bảng **PHANCONG** khi người dùng truy cập vào hệ thống và thực hiện việc sửa đổi thông tin cột **THOIGIAN**.

#### Những người đã đọc trên trường LUONG và PHUCAP của người khác:

❖ Phương thức sử dụng: FGA Audit.

❖ Cách thức cụ thể:

• Sử dụng gói **DBMS\_FGA**.

• Gọi thủ tục **ADD\_POLICY** và truyền các tham số để áp dụng chính sách audit lên bảng **NHANVIEN** theo yêu cầu:

|  |  |
| --- | --- |
| **OBJECT\_SCHEMA** | COMPANY |
| **OBJECT\_NAME** | NHANVIEN |
| **POLICY\_NAME** | B\_AUDIT |
| **AUDIT\_COLUMN** | LUONG, PHUCAP |
| **AUDIT\_CONDITION** | NHANVIEN.MANV != SYS\_CONTEXT (''USERENV'', ''SESSION\_USER'') |
| **STATEMENT\_TYPES** | SELECT |
| **ENABLE** | TRUE |

⇨ Chính sách sẽ ghi lại các hoạt động **SELECT** trên cột **LUONG** và **PHUCAP** của bảng **NHANVIEN** khi mà người dùng truy cập có **USERNAME** khác với **MANV** trong bảng **NHANVIEN** mà người đó đang cố gắng **SELECT**.

#### Những người không thuộc vai trò “Tài chính” nhưng cập nhật thành công thuộc tính ‘LUONG’ và ‘PHUCAP’

❖ Phương thức sử dụng: Trigger Audit

❖ Cách thức cụ thể:

• Tạo bảng **‘aud\_LUONG’**: Bảng này được tạo để lưu trữ các bản ghi kiểm tra. Nó bao gồm các cột để lưu trữ thông tin như tên người dùng, loại hành động (insert, update, delete), NHANVIEN bị ảnh hưởng, tên cột, Call Stack, ID Client, giá trị cũ, giá trị mới và ngày thực hiện hành động.

• Thủ tục **‘audit\_LUONG’:** Thủ tục này được sử dụng để chèn các bản ghi kiểm tra vào bảng ‘**aud\_LUONG**’. Nó nhận các tham số như tên người dùng, loại hành động, **NHANVIEN**, tên cột, giá trị cũ và giá trị mới. Thủ tục sử dụng hàm **DBMS\_UTILITY.format\_call\_stack** để lấy **Call Stack** và **SYS\_CONTEXT('userenv', 'client\_identifier')** để lấy **ID Client**.

• Thủ tục ‘**show\_aud\_LUONG\_PHUCAP**’: Thủ tục này được sử dụng để hiển thị các bản ghi kiểm tra từ bảng **‘aud\_LUONG’**. Nó truy xuất các bản ghi từ bảng theo thứ tự giảm dần của ngày hành động và xuất thông tin liên quan bằng cách sử dụng gói ‘**DBMS\_OUTPUT**’.

• Trigger ‘**update\_LUONG\_trig**’: Trigger này được kích hoạt trước khi thực hiện cập nhật trên cột ‘**LUONG**’ của bảng ‘**NHANVIEN**’. Nó kiểm tra xem người dùng có vai trò 'TC' (như được chỉ định trong bảng ‘**DBA\_ROLE\_PRIVS**’) hoặc người dùng '**COMPANY**' hay không. Nếu điều kiện được đáp ứng, thủ tục ‘**audit\_LUONG**’ được gọi với các tham số cần thiết để chèn một bản ghi kiểm tra cho việc cập nhật.

• Trigger ‘**update\_PHUCAP\_trig**’: Trigger này tương tự như trigger trước, nhưng được kích hoạt trước khi thực hiện cập nhật trên cột ‘**PHUCAP**’ của bảng ‘**NHANVIEN**’. Nó cũng gọi thủ tục ‘**audit\_LUONG**’ để chèn một bản ghi kiểm tra.

#### Kiểm tra nhật kí hệ thống

- Kiểm tra nhật kí hệ thống bằng các sử dụng view **UNIFIED\_AUDIT\_TRAIL**.

- Khi mà **unified auditing** được kích hoạt trên Oracle thì những bản ghi kiểm tra sẽ được khi vào view này.

- Nhóm chúng em đã sử dụng chính sách FGA để thực hiện việc khi vết. Để có thể truy cập được view này thfi người dùng đã được cấp role **AUDIT\_ADMIN** và **AUDIT\_VIEWER**.

**- SELECT** \* **FROM** UNIFIED\_AUDIT\_TRAIL **WHERE** AUDIT\_TYPE = 'FineGrainedAudit' để có thể lọc ra các bạn ghi sử dụng chính sách FGA.

#### Giao diện

##### Màn hình sử dụng **Standard Audit**:

Ở chức năng này, giao diện sẽ hiển thị chi tiết để kiểm tra nhật ký hệ thống, cụ thể sẽ có các thông tin đáng quan tâm như sau:

• **SESSIONID:** ID phiên của người dùng trong cơ sở dữ liệu.

• **OS\_USERNAME**: Tên người dùng trên hệ thống điều hành.

• **USERHOST**: Tên máy tính của người dùng.

• **INSTANCE\_ID**: ID của phiên cơ sở dữ liệu.

• **DBID**: ID của cơ sở dữ liệu.

• **AUTHENTICATION\_TYPE**: Loại xác thực (ví dụ: PASSWORD, EXTERNAL, KERBEROS)

• **DBUSERNAME**: Tên người dùng trên cơ sở dữ liệu

• **CLIENT\_PROGRAM\_NAME**: Tên chương trình sử dụng kết nối đến cơ sở dữ liệu.

• **ENTRY\_ID**: ID của mục nhập trong bảng UNIFIED\_AUDIT\_TRAIL.

• **STATEMENT\_ID**: ID của câu lệnh SQL được thực thi.

• **EVENT\_TIMESTAMP**: Thời điểm xảy ra sự kiện trong múi giờ địa phương.

**• EVENT\_TIMESTAMP\_UTC**: Thời điểm xảy ra sự kiện trong múi giờ UTC.

• **ACTION\_NAME**: Tên hoạt động được thực hiện (ví dụ: SELECT, INSERT, UPDATE, DELETE)

• **OS\_PROCESS**: ID quá trình hệ thống.

• **SCN**: Số bảo đảm cho thời điểm truy cập.

• **EXECUTION\_ID**: ID của phiên thực thi.

• **OBJECT\_SCHEMA**: Tên schema của đối tượng được truy cập.

• **OBJECT\_NAME**: Tên của đối tượng được truy cập.

• **SQL\_TEXT**: Câu lệnh SQL được thực thi.

• **CURRENT\_USER**: Người dùng hiện tại trên cơ sở dữ liệu.

• **ADDITIONAL\_INFO**: Thông tin bổ sung về sự kiện.

• **UNIFIED\_AUDIT\_POLICIES**: Tên chính sách kiểm tra toàn diện được áp dụng.

• **FGA\_POLICY\_NAME**: Tên chính sách ghi lại truy cập bảo vệ dữ liệu (Fine-Grained Auditing Policy) nếu có.

A screenshot of a computer

Description automatically generated

Hình . Giao diện chức năng Standard Audit

##### Màn hình sử dụng **Fine Grained Audit**:

A screenshot of a computer

Description automatically generated

Hình . Giao diện chức năng **Fine Gained Audit**

Với chức năng này, màn hình sẽ hiển thị chi tiết các thông tin tương tự chức năng Standard Audit. Tuy nhiên, màn hình chỉ hiện thị thông tin ghi vết các hoạt động bằng chính sách FGA (Fine-Grained Auditing Policy) được yêu cầu cài đặt trong đồ án:

- Những người đã cập nhật trường THOIGIAN trong quan hệ PHANCONG.

- Những người đã đọc trên trường LUONG và PHUCAP của người khác.

##### Màn hình sử dụng Trigger Audit

A screenshot of a computer

Description automatically generated

Hình . Giao diện chức năng **Trigger Audit**

Trong chức năng này, màn hình sẽ hiện thông tin ghi vết của hoạt động: Một người không thuộc vai trò “Tài chính” nhưng đã cập nhật thành công trên trường LUONG và PHUCAP.

Cụ thể, sẽ có các thông tin đáng quan tâm như:

• **username**: Tên người dùng thực hiện hoạt động này trên cơ sở dữ liệu.

• **action**: Hành động được thực hiện trên bảng LUONG, ví dụ như "INSERT", "UPDATE", hoặc "DELETE" (ở đây là “UPDATE”).

• **nhanvien**: Mã nhân viên liên quan đến hoạt động này.

• **column\_name**: Tên cột được thay đổi trong hoạt động "UPDATE".

• **call\_stack**: Chuỗi gọi hàm được lưu trữ khi thực hiện hoạt động trên cơ sở dữ liệu.

• **client\_id**: ID của khách hàng thực hiện hoạt động này.

• **old\_value**: Giá trị cũ của cột được thay đổi trong hoạt động "UPDATE".

• **new\_value**: Giá trị mới của cột được thay đổi trong hoạt động "UPDATE".

• **action\_date**: Ngày giờ thực hiện hành động trên cơ sở dữ liệu.

# HƯỚNG DẪN SỬ DỤNG

- Hướng dẫn sử dụng được trình bày cụ thể trong file **“23H3T-16-PH1-PH2-Guide.pdf”**.

- Demo sử dụng được trình bày trong file “**23H3T-16-PH1-PH2-demo.pdf**”.

# TÀI LIỆU THAM KHẢO

1. github.com. 2023. *GitHub - hduylam31/ATBM-trong-HTTT: Đồ án thực hành môn an toàn và bảo mật dữ liệu trong hệ thống thông tin.*[ONLINE] Available at: <https://github.com/hduylam31/ATBM-trong-HTTT/tree/main>. [Accessed 29 June 2023].
2. github.com. 2023. *GitHub - tuanhbui/ATBM: sc.*[ONLINE] Available at: <https://github.com/tuanhbui/ATBM>. [Accessed 29 June 2023].
3. docs.oracle.com. 2023. *Oracle Database Database Concepts, 21c.*[ONLINE] Available at: [Database Concepts (oracle.com)](https://docs.oracle.com/en/database/oracle/oracle-database/21/cncpt/index.html#Oracle%C2%AE-Database). [Accessed 29 June 2023].