

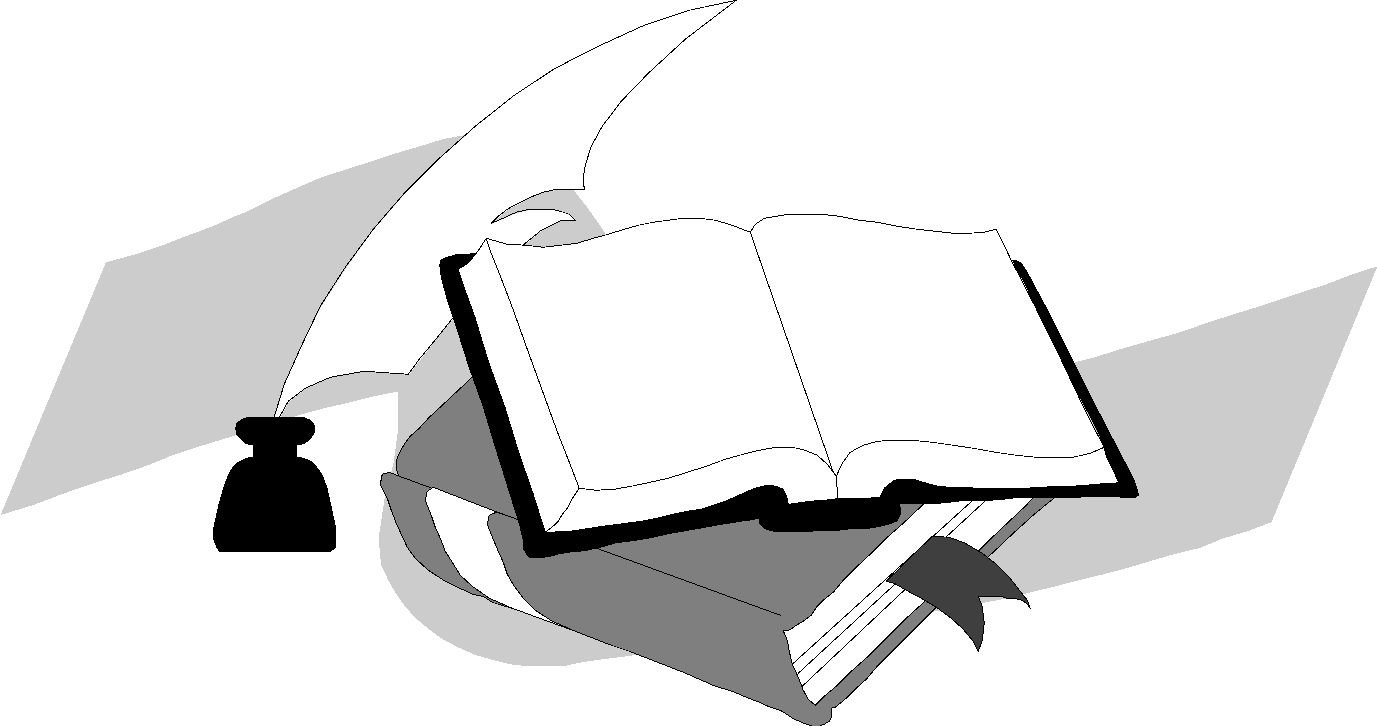
****



**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**BÁO CÁO**

**HỌC PHẦN: QUẢN TRỊ CƠ SỞ DỮ LIỆU**



**BÁO CÁO BÀI TẬP NHÓM**

**Giáo viên hướng dẫn : Cao Thị Nhâm**

**Lớp : 46K21.2**

**Nhóm : 9**

**Sinh viên thực hiện : Phạm Tây Hồ**

**Trần Quốc Hải**

**Nguyễn Khánh Vy**

**Phan Thị Thu Thảo**

**Nguyễn Thị Ngọc Giàu**

**Nguyễn Thị Hoàng Linh**



***Đà Nẵng, Ngày 2 tháng 12 năm 2022***

Muc Lục

[**1. Hóa đơn nhóm chọn** 3](#_Toc120864868)

[**2. Thiết kế cơ sở dữ liệu** 7](#_Toc120864869)

[**2.1. Thiết kế cơ sở dữ liệu mức khái niệm** 7](#_Toc120864870)

[**2.2. Thiết kế cơ sở dữ liệu mức logic** 8](#_Toc120864871)

[**2.3. Thiết kế cơ sở dữ liệu mức vật lý** 8](#_Toc120864872)

[**3. Xây dựng cơ sở dữ liệu** 10](#_Toc120864873)

[**4. Xác định và tạo index cho các thuộc tính** 20](#_Toc120864874)

[**5. Xây dựng cơ chế bảo mật tương ứng cho cơ sở dữ liệu vừa tạo** 22](#_Toc120864875)

[**6. Xây dựng cơ chế backup dữ liệu phù hợp cho cơ sở dữ liệu vừa tạo** 28](#_Toc120864876)

[**7. Phát triển ứng dụng (C#)** 30](#_Toc120864877)

[**7.1. Form Đăng nhập** 30](#_Toc120864878)

[**7.2. Form Quản lý** 31](#_Toc120864879)

[**7.3. Form Menu** 31](#_Toc120864880)

[**7.4. Form Hóa đơn** 32](#_Toc120864881)

[**7.5. Form Chi tiết hóa đơn** 33](#_Toc120864882)

[**7.6. Form Nhân viên** 34](#_Toc120864883)

[**7.7. Form Khách Hàng** 35](#_Toc120864884)

[**7.8. Form Phiếu nhập hàng** 36](#_Toc120864885)

[**7.9 Form Chi tiết nhập hàng** 37](#_Toc120864886)

[**7.10. Form Tài khoản** 38](#_Toc120864887)

[**8. Phương án giải quyết vấn đề dữ liệu lớn** 39](#_Toc120864888)

[**9. Đề phòng phương án hệ thống bị tấn công bằng SQL Injection** 40](#_Toc120864889)

[9.1. SQL Injection là gì? 40](#_Toc120864890)

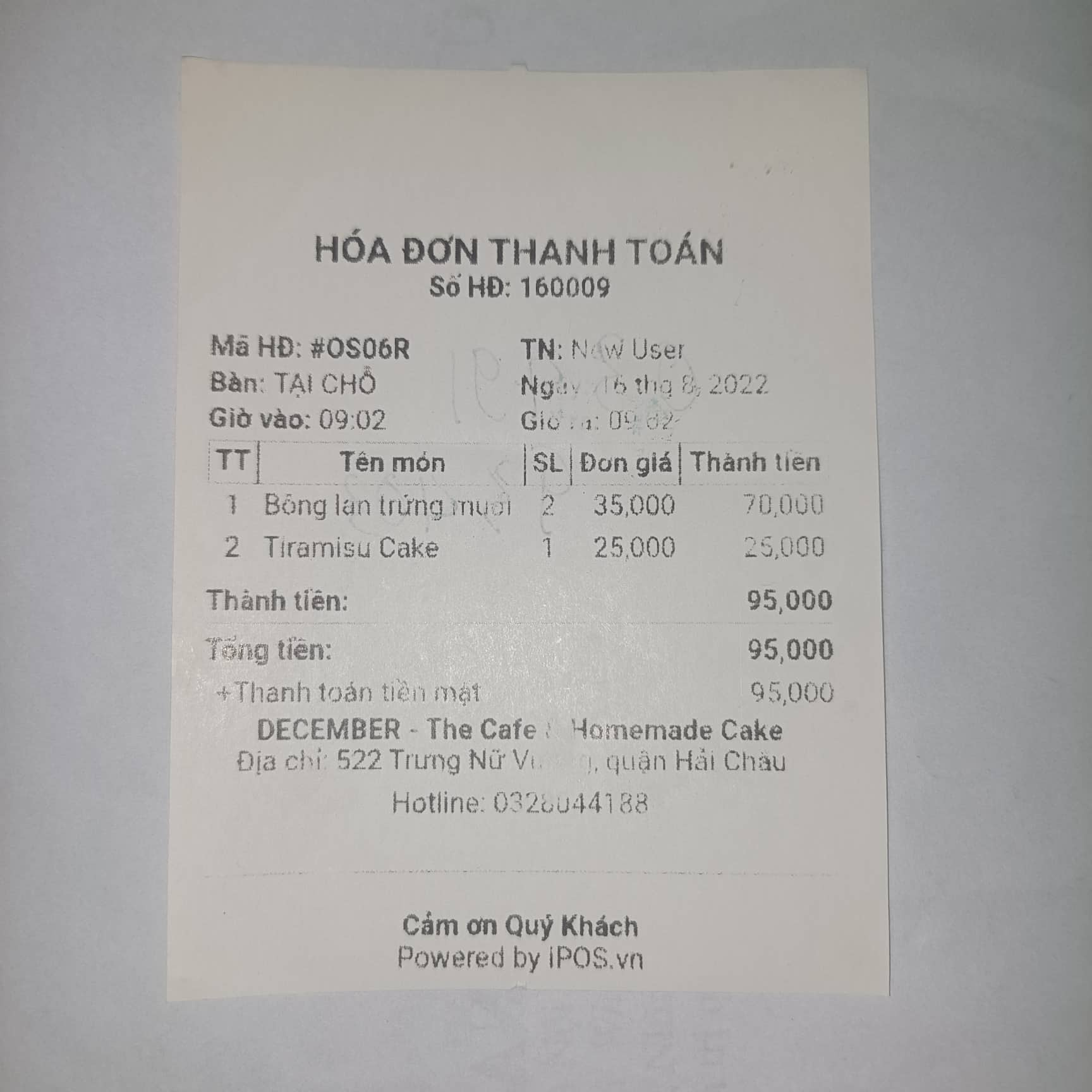
[9.2. Một số phương án phòng chống. 40](#_Toc120864891)

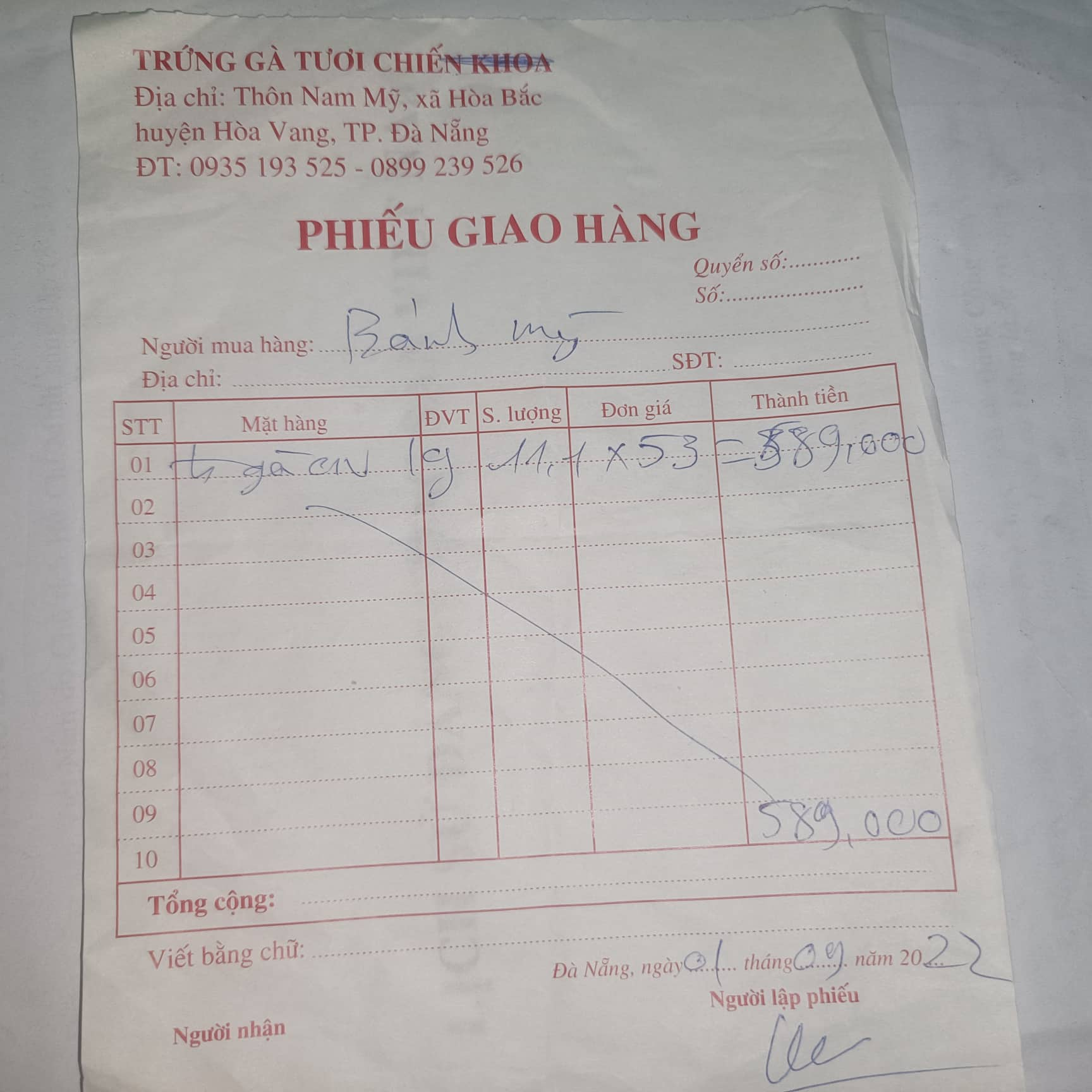
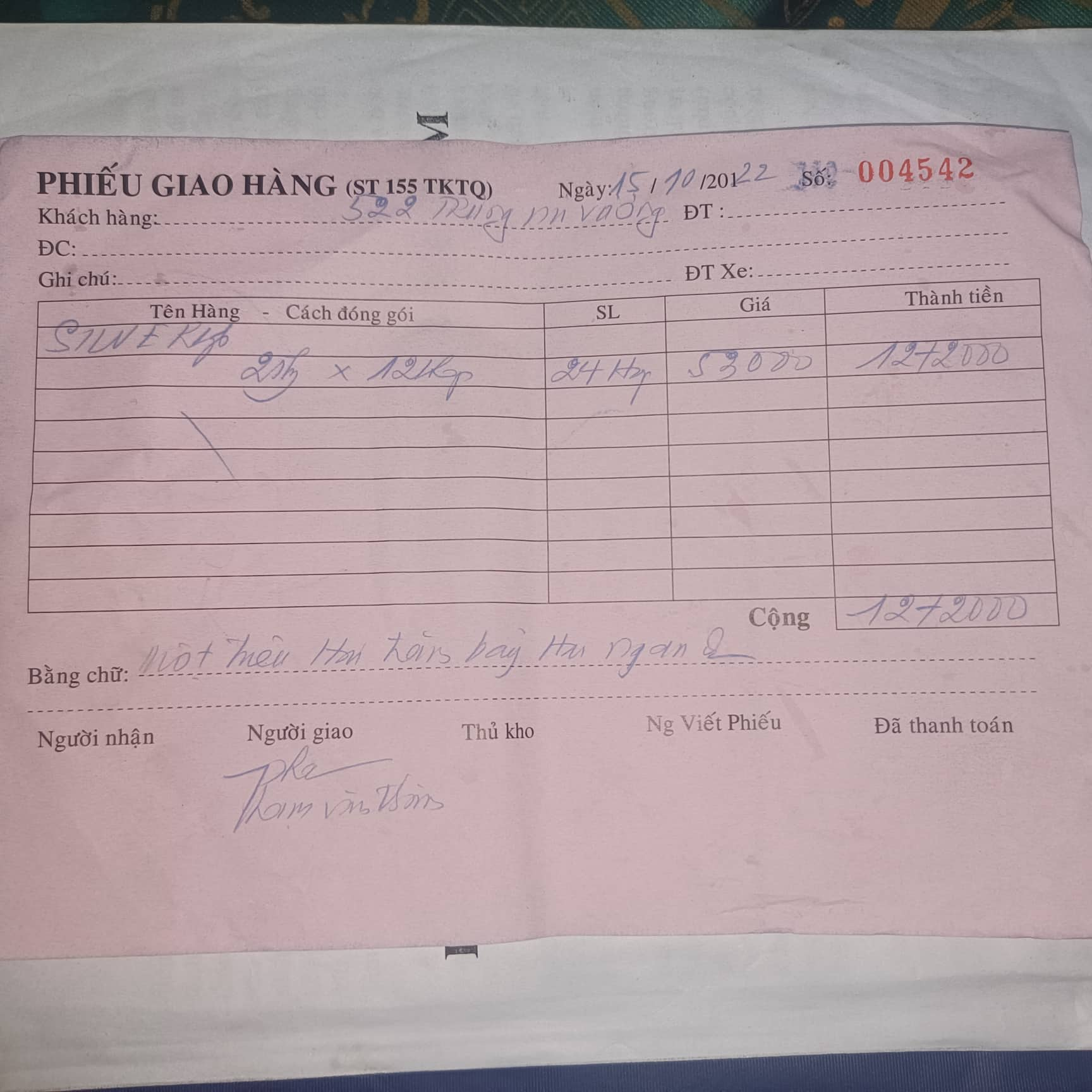
**Đề tài**: Hệ thống quản lý bán hàng

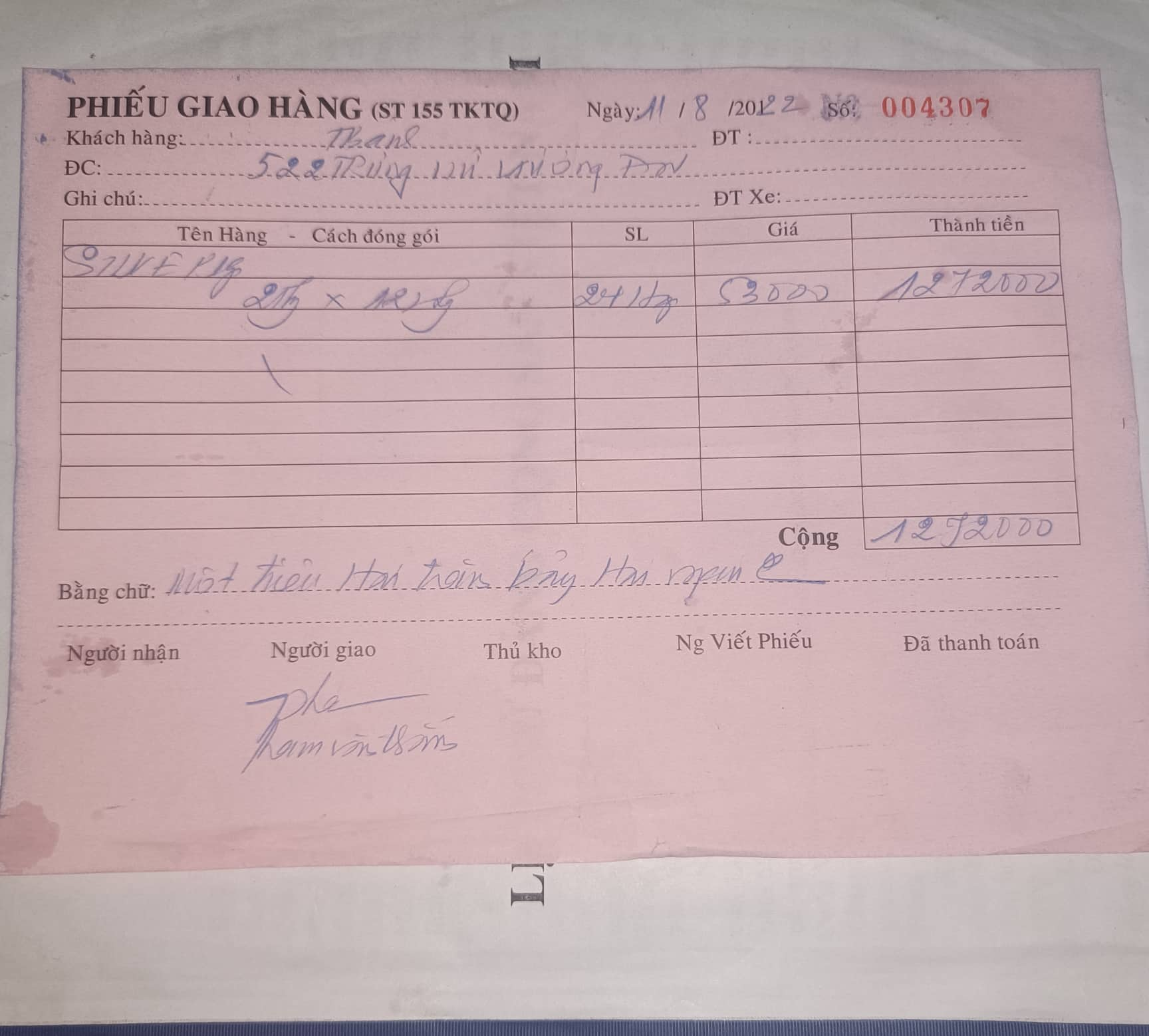
Cơ sở khảo sát: Coffee December

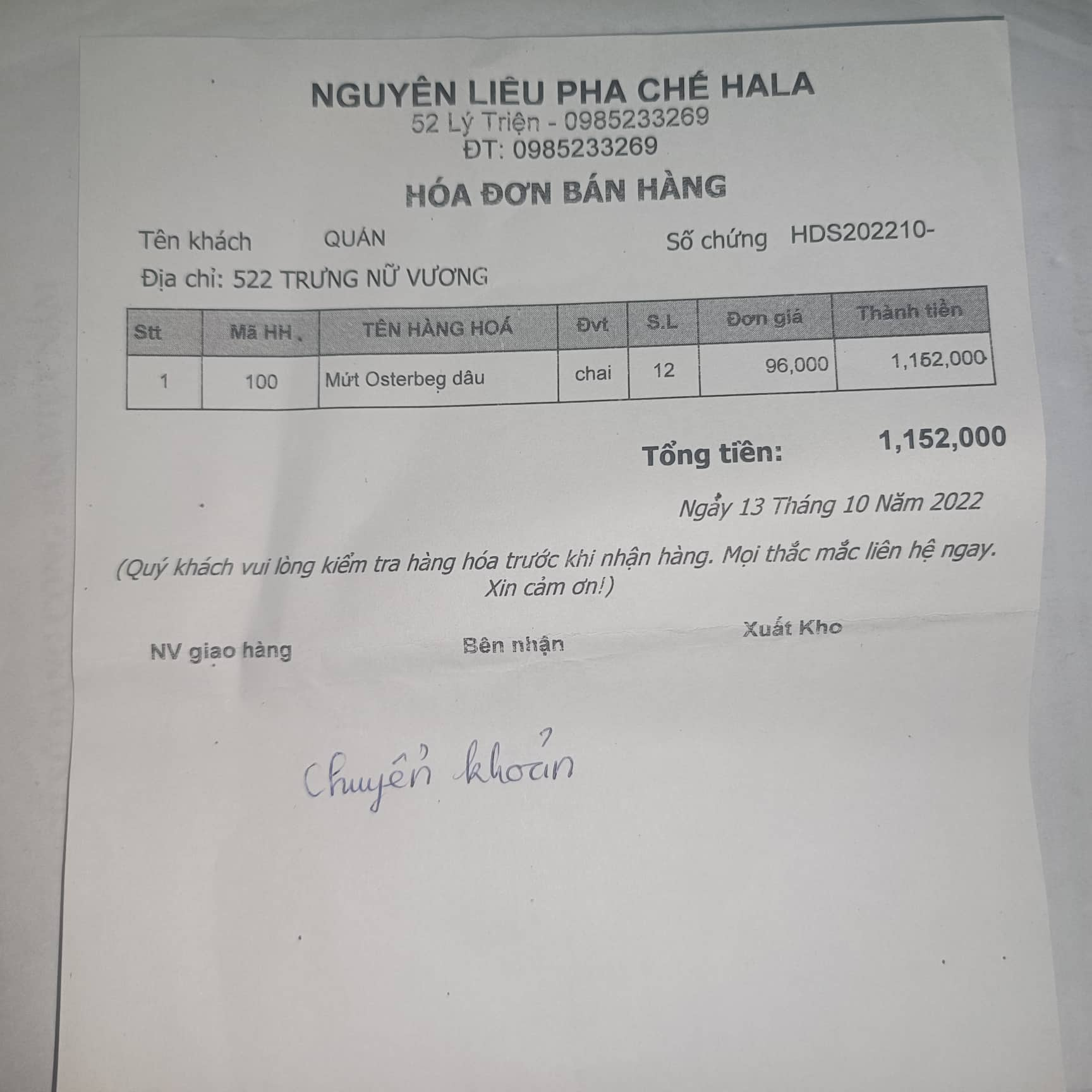
Địa chỉ: 522 Trưng Nữ Vương- TP Đà Nẵng

# **1. Hóa đơn nhóm chọn**

****

****

****

****

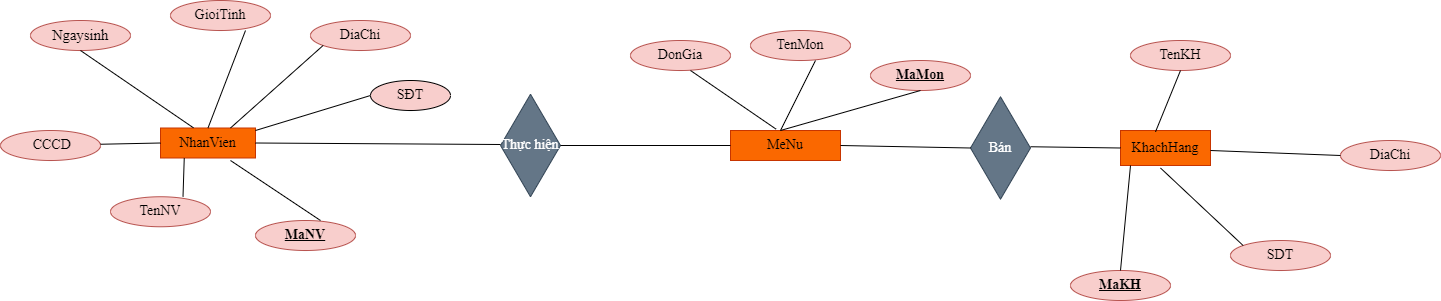
# **2. Thiết kế cơ sở dữ liệu**

## **2.1. Thiết kế cơ sở dữ liệu mức khái niệm**

Xây dựng ER cho hóa đơn bán hàng

Các thực thể:

* NHANVIEN (**MaNV**, TenNV, CCCD, Ngaysinh, GioiTinh, DiaChi, SĐT)
* KHACHHANG (**MaKH**, TenKH, SDT, Diachi)
* MENU (**MaMon**, TenMon, DonGia)
* Quan hệ:



## **2.2. Thiết kế cơ sở dữ liệu mức logic**

* Sơ đồ ràng buộc quan hệ:

Diagram

Description automatically generated

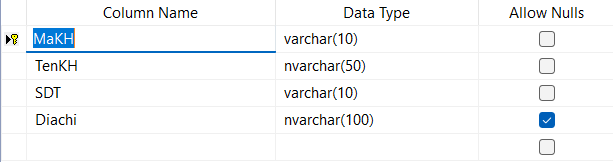
## **2.3. Thiết kế cơ sở dữ liệu mức vật lý**

* **Bảng Tài khoản**

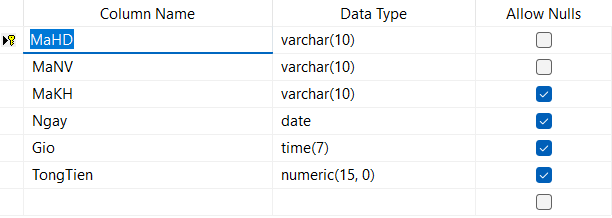
**Graphical user interface, application, table

Description automatically generated**

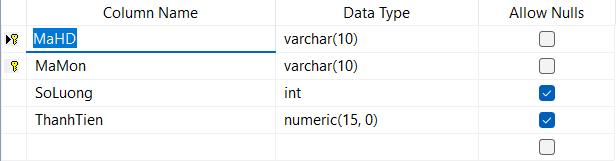
* **Bảng Khách hàng**



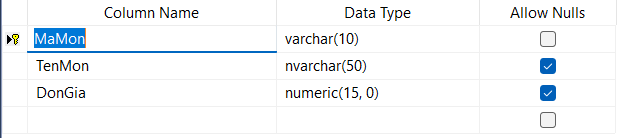
* **Bảng Hóa đơn**



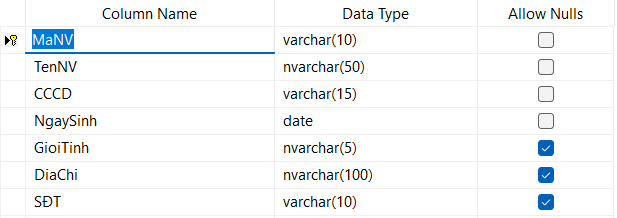
* **Bảng Chi tiết hóa đơn**



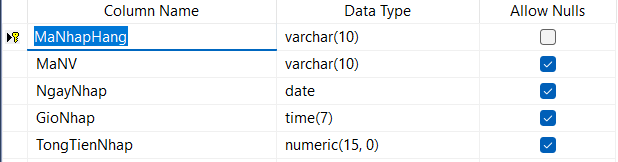
* **Bảng Menu**



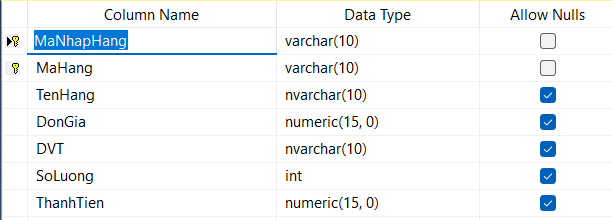
* **Bảng Nhân viên**



* **Bảng Phiếu nhập hàng**



* **Bảng Chi tiết nhập hàng**



# **3. Xây dựng cơ sở dữ liệu**

Tạo dữ liệu cho bảng TAIKHOAN

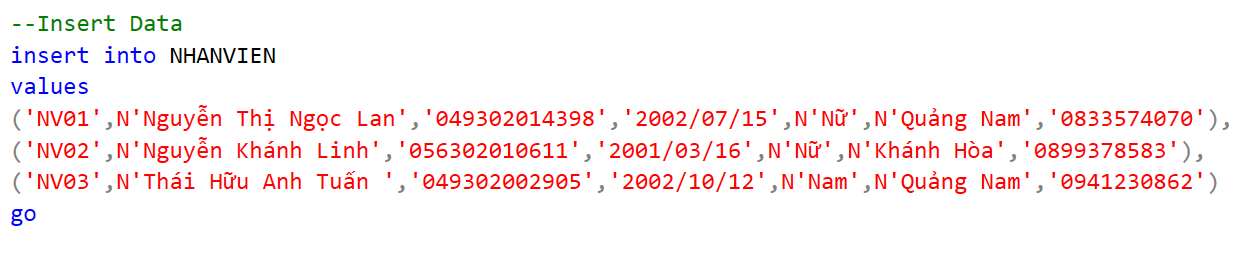
**Graphical user interface, text, application

Description automatically generated**

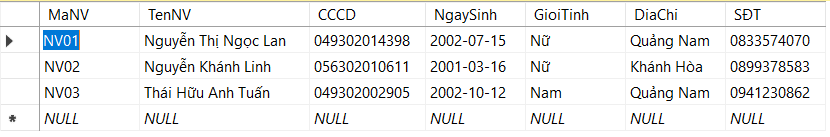
Kết quả nhập dữ liệu

**Table

Description automatically generated with medium confidence**

Tạo dữ liệu cho bảng NHANVIEN 

Kết quả nhập dữ liệu



Tạo dữ liệu cho bảng PHIEUNHAPHANG

Text

Description automatically generated

Kết quả nhập dữ liệu bảng PHIEUNHAPHANG

Table

Description automatically generated

Tạo dữ liệu cho bảng CHITIETNHAPHANG

Text

Description automatically generated with medium confidence

Tạo trigger sau khi Insert CHITIETNHAPHANG

→ Update ThanhTien ở bảng CHITIETNHAPHANG

→ Update TongTienNhap ở bảng PHIEUNHAPHANG

Graphical user interface, text, application

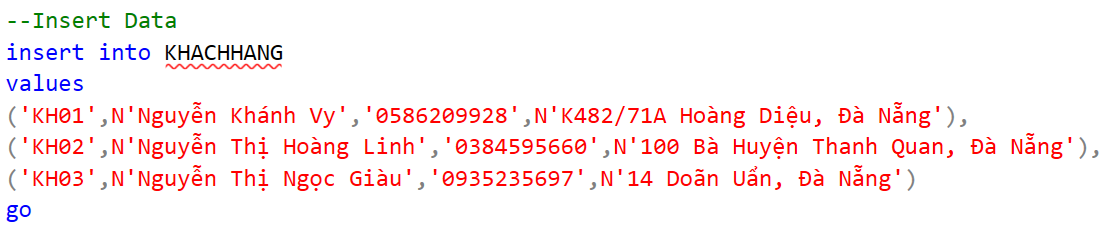
Description automatically generated

Kết quả nhập dữ liệu bảng CHITIETNHAPHANG

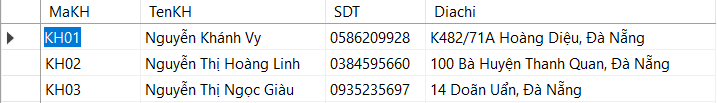
Table

Description automatically generated

Tạo dữ liệu bảng KHACHHANG



Kết quả nhập dữ liệu bảng KHACHHANG



Tạo dữ liệu bảng MENU

A picture containing table

Description automatically generated

A picture containing table

Description automatically generated

Kết quả nhập dữ liệu bảng MENU

Table

Description automatically generated

Tạo dữ liệu bảng HOADON

Text

Description automatically generated

Kết quả nhập dữ liệu bảng HOADON

Table

Description automatically generated

Tạo dữ liệu cho bảng CHITIETHOADON

Table

Description automatically generated

Tạo trigger sau khi Insert CHITIETHOADON

→ Update ThanhTien ở bảng CHITIETHOADON

→ Update TongTien ở bảng HOADON

Text

Description automatically generated

Kết quả nhập dữ liệu bảng CHITIETHOADON

Table

Description automatically generated

Tạo trigger sau khi Update CHITIETHOADON

→ Update ThanhTien ở bảng CHITIETHOADON

→ Update TongTien ở bảng HOADON

Graphical user interface, text, application

Description automatically generated

Tạo trigger sau khi Update CHITIETNHAPHANG

→ Update ThanhTien ở bảng CHITIETNHAPHANG

→ Update TongTienNhap ở bảng PHIEUNHAPHANG

Text

Description automatically generated

# **4. Xác định và tạo index cho các thuộc tính**

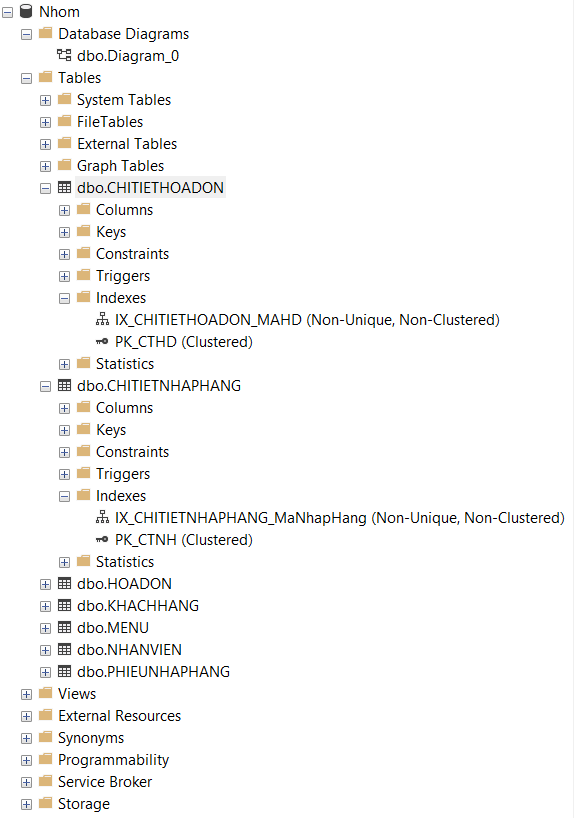
Index là một cấu trúc liên kết với một bảng hoặc một view dùng để tăng tốc độ truy vấn dữ liệu. Index chứa các khóa được tạo từ một hay nhiều cột và được lưu trữ dưới dạng B-tree.Nó cho phép SQL Server có thể tìm thấy các row liên quan một cách nhanh chóng và hiệu quả nhất. Nếu sử dụng không đúng cách nó sẽ làm chậm tốc độ update, insert, delete trong cơ sở dữ liệu.

Có 2 loại Index là Clustered Index và Non Clustered Index.

Trong CSDL của nhóm, nhóm đã tạo 2 Non Clustered Index.

Dùng cho cột MaHD trong bảng CHITIETHOADON và cột MaNhapHang trong bảng CHITIETNHAPHANG. Bởi vì số lần dùng đến dữ liệu 2 cột này nhiều và 2 cột này không có giá trị Null trong các bảng chứa nó.





# **5. Xây dựng cơ chế bảo mật tương ứng cho cơ sở dữ liệu vừa tạo**

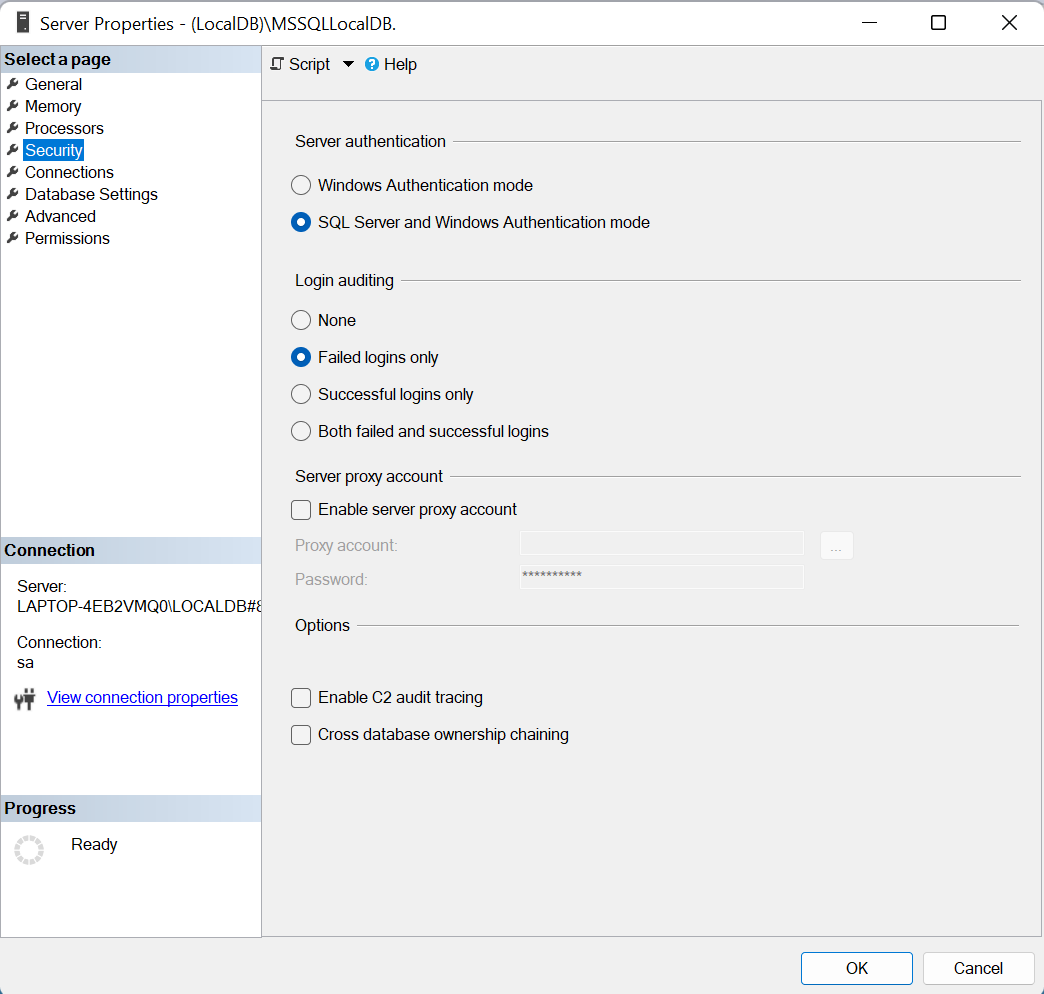
Authentication: xác thực người dùng ở cấp ứng dụng

Nhóm đã tạo account bên trong csdl(quyết định người dùng có quyền connect vào

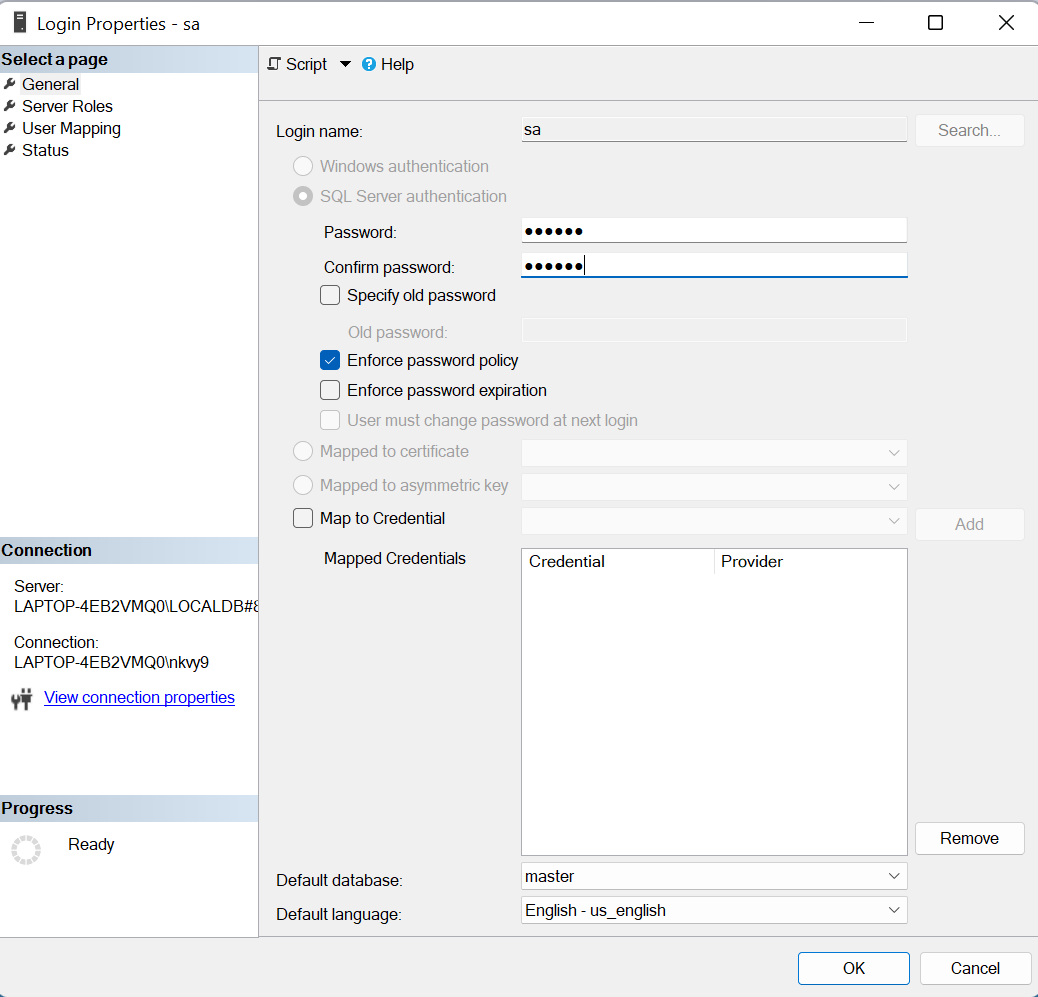
hệ thống không) & authority(phân quyền cho người dùng)

Quá trình thực hiện :

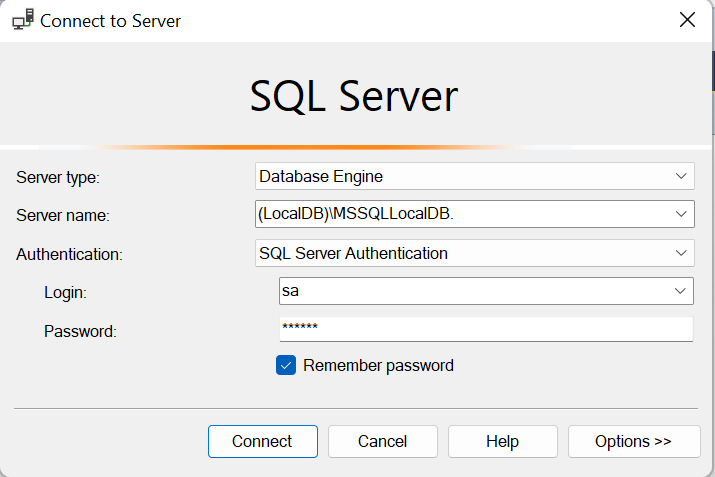
**Bước 1: kích hoạt chế độ Sql server Authentication**

****

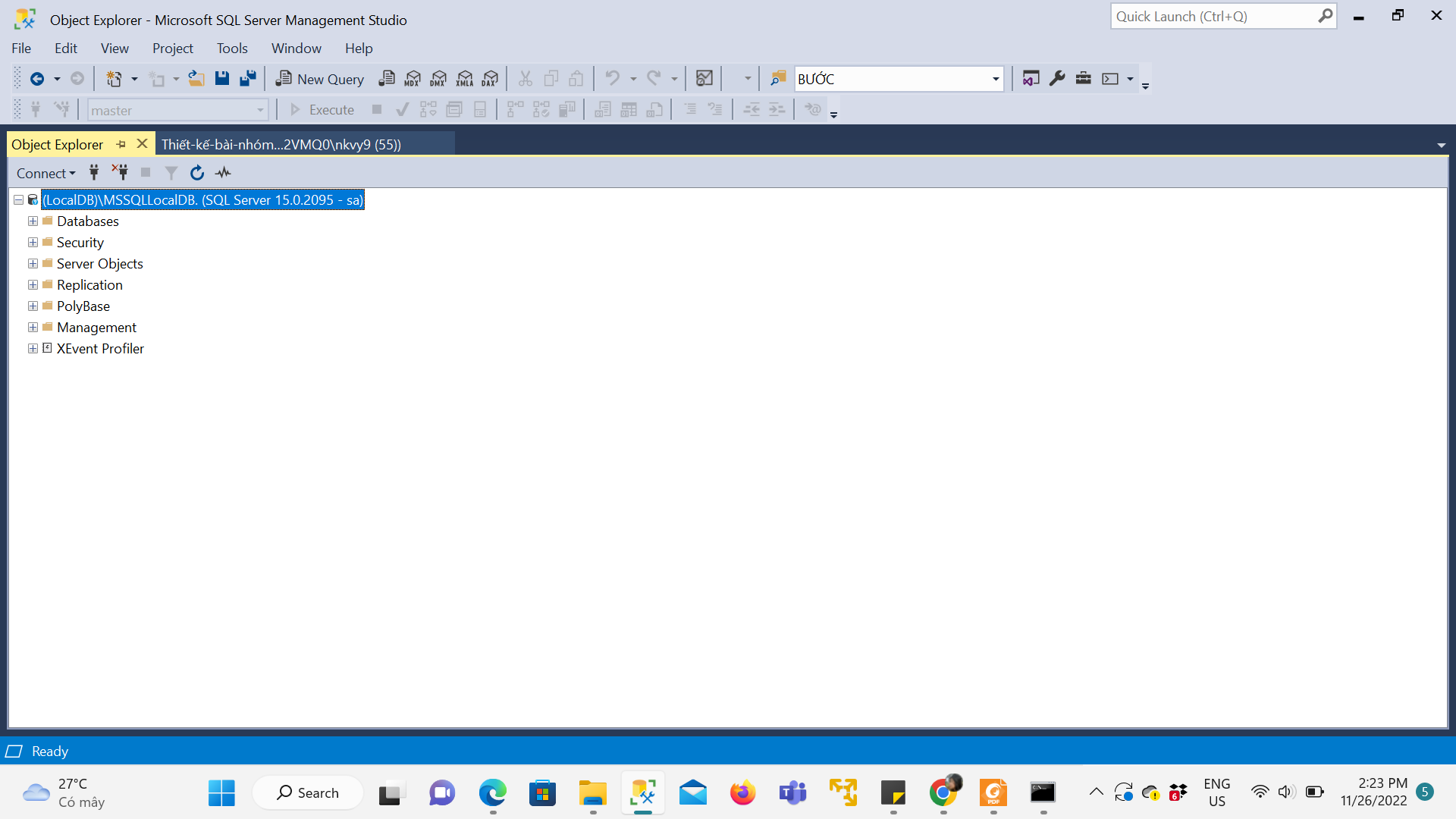
**Bước 2: Tạo tài khoản Login với tên tài khoản là SA**

****

**Bước 3: Kết quả sau khi tạo, người dùng muốn vào CSDL thì phải đăng nhập vào tài khoản**

****

**Bước 4: Đăng nhập thành công với tài khoản vừa tạo**

****

Data security:

Mã hoá là một phương pháp quan trọng nhằm bảo mật dữ liệu. Những dữ liệu

nhạy cảm như số CCCD, số thẻ tín dụng, mật khẩu và thông tin cá nhân như số

điện thoại khách hàng,… cần phải được bảo vệ trước vô vàn mối nguy hiểm tấn

công hiện nay.

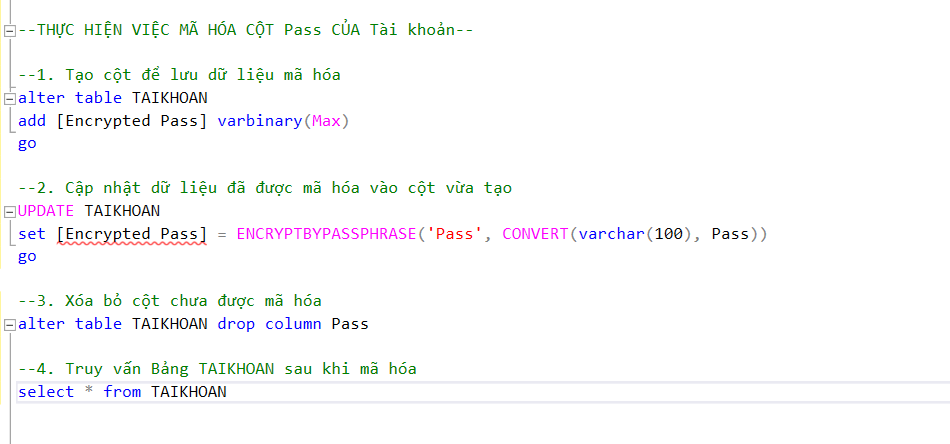
Nhóm đã sử dụng phương pháp mã hóa đối xứng 2 chiều cho cơ sở dữ liệu vừa

tạo bằng hàm mã hóa 2 chiều EncryptByPassPhrase trong SQL server.

Thực hiện việc mã hóa thông tin của cột số điện thoại trong bảng Khách Hàng

thông qua phương pháp mã hóa bằng mật khẩu

THỰC HIỆN BẰNG CODE



Sau khi mã hóa xong, truy vấn dữ liệu trong bảng KHACHHANG, ta được kết

quả sau:

Graphical user interface, text, application, Word

Description automatically generated

Giải mã dữ liệu trên bảng thông qua hàm Decryptbypassphrase



Kết quả sau khi giải mã thành công cột SĐT trong bảng KHACHHANG:

Graphical user interface, text, application

Description automatically generated

SQL Server sẽ trả lại kết quả là NULL nếu mậtt khẩu sai

THỰC HIỆN BẰNG GIAO DIỆN

Mã hóa

A picture containing table

Description automatically generated

Graphical user interface, application

Description automatically generated

Kết quả sau khi mã hóa

Graphical user interface, text, application

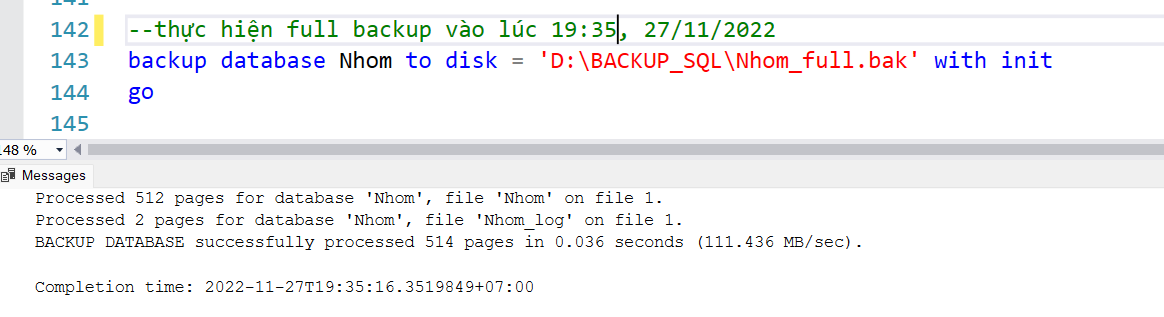
Description automatically generated

# **6. Xây dựng cơ chế backup dữ liệu phù hợp cho cơ sở dữ liệu vừa tạo**

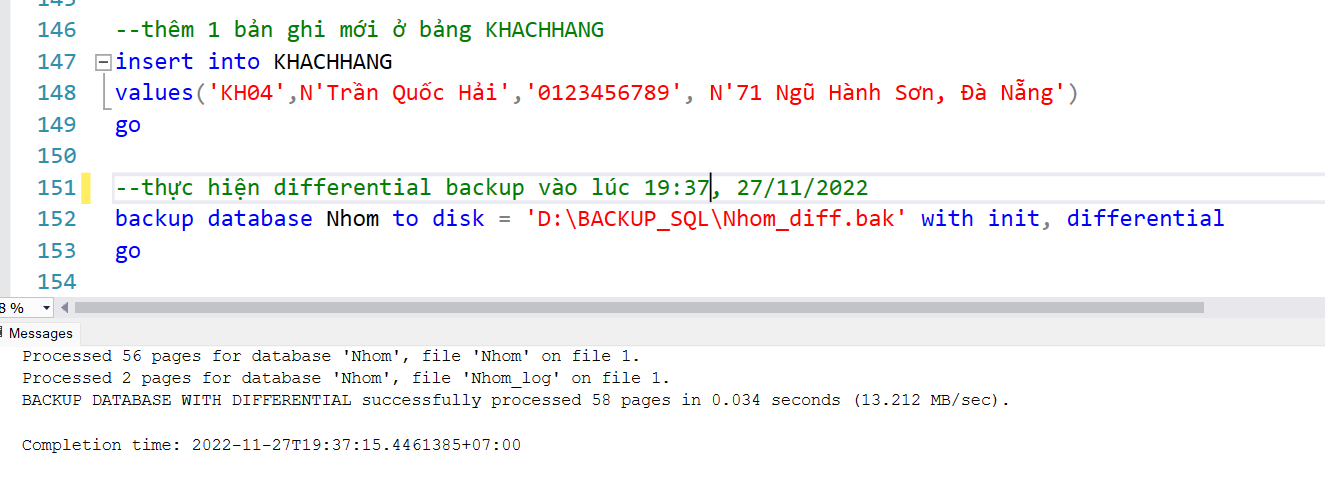
Backup là 1 hình thức sao chép lại toàn bộ đoạn dữ liệu trong server có thể lưu trữ và nhớ dữ liệu của bạn. Lưu trữ nó ở 1 hay nhiều thiết bị có chức năng lưu trữ khác để làm dữ liệu dự phòng. Để nhằm mục đích đảm bảo người dùng sẽ không mất dữ liệu hoàn toàn và vĩnh viễn.

Vì dữ liệu là những thông tin được bảo mật và nó ảnh hưởng trực tiếp đến hoạt động kinh doanh của doanh nghiệp. Nhưng dữ liệu cá nhân hay là dữ liệu của doanh nghiệp đều có nguy cơ tiềm ẩn bị mất do nhiều lý do khác nhau như máy chủ bị hacker tấn công, máy tính bị hỏng,..Trong trường hợp khi bị hacker cướp dữ liệu tấn công nhằm mục đích thương mại, trừ những thông tin mật thì cần phải được mua lại. Còn toàn bộ dữ liệu quan trọng đều có khả năng giữ lại bằng những biện pháp backup sao lưu. Vậy nên, backup dữ liệu là 1 việc cần thiết mà hầu hết người sử dụng nào cũng thực hiện, công việc đơn giản, không mất quá nhiều thời gian nhưng mang lại hiệu quả cao và hữu ích.

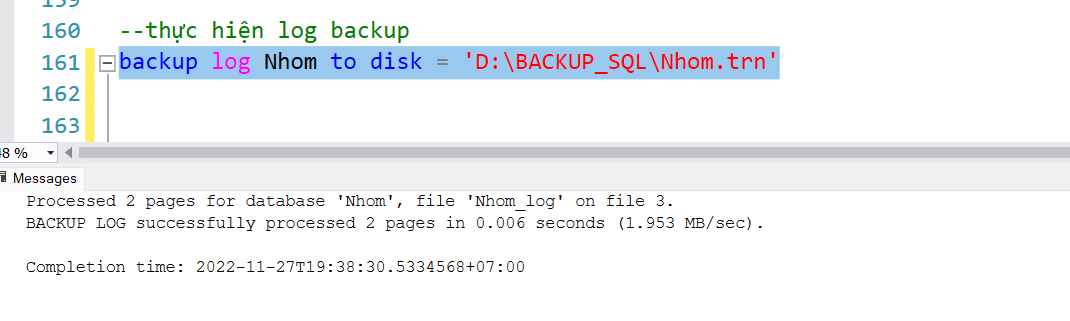
* **Full Backup**

****

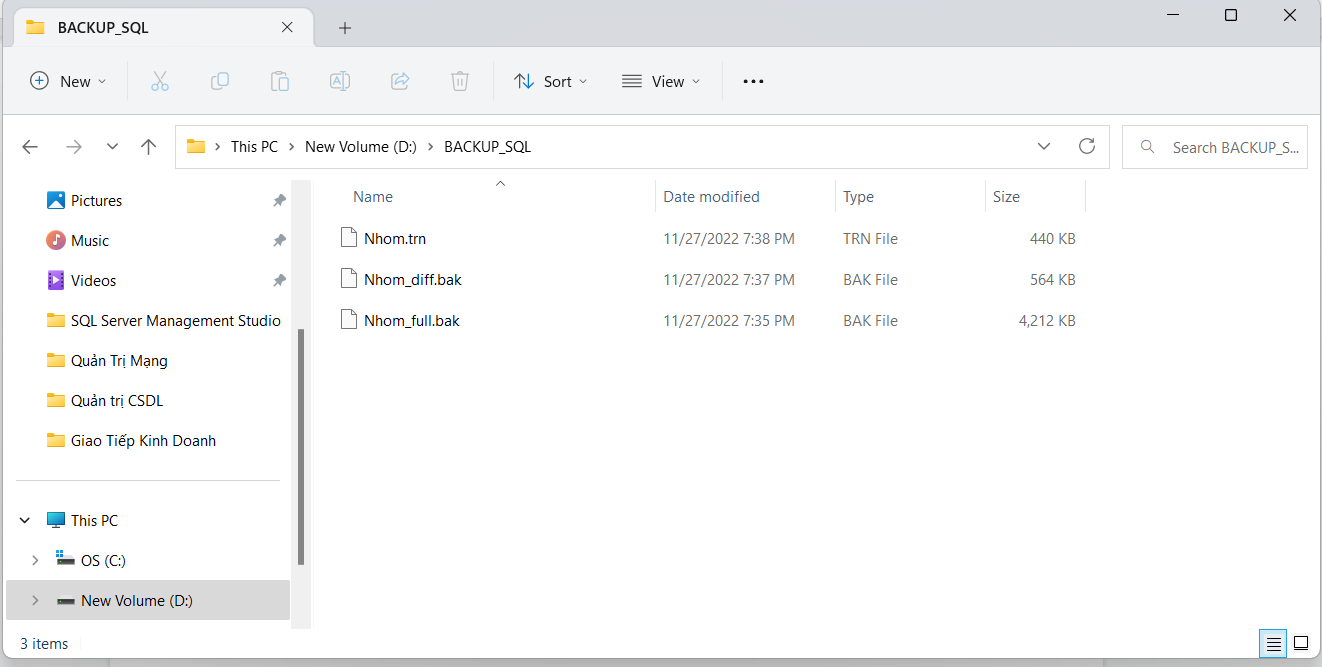
* **Differential Backup**

****

* **Log Backup**

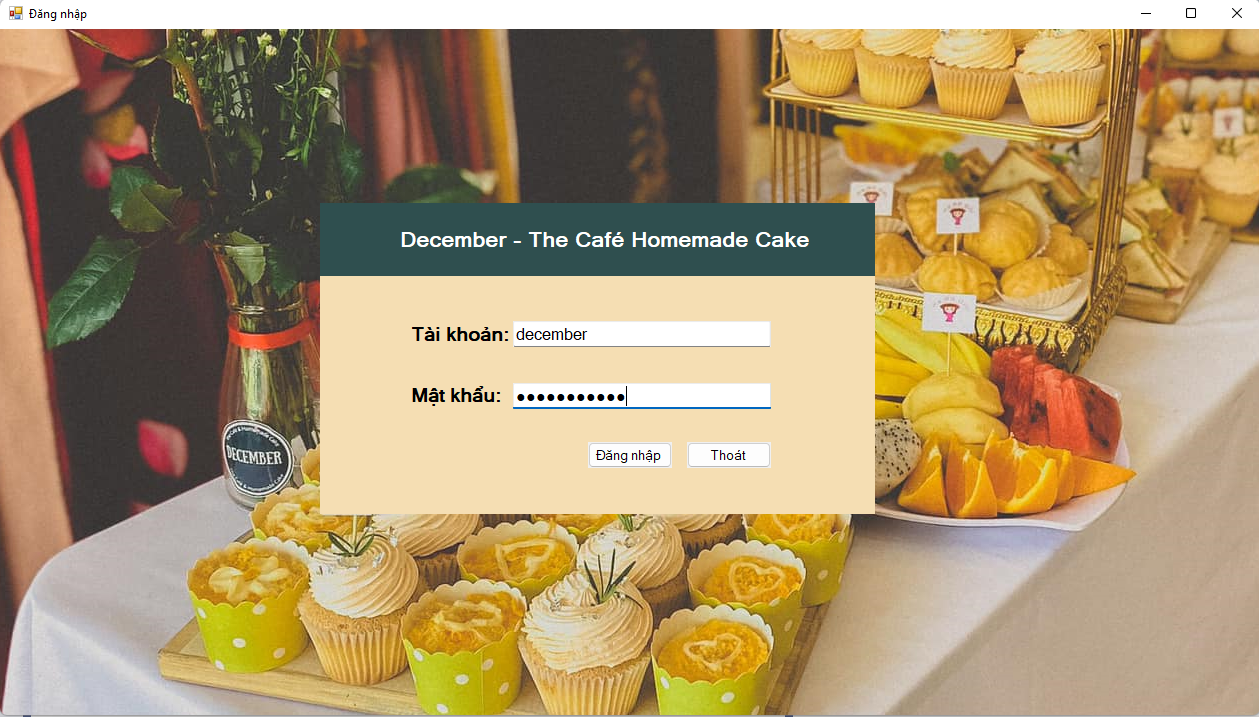
****

* **Kiểm tra kết quả backup**

****

# **7. Phát triển ứng dụng (C#)**

## **7.1. Form Đăng nhập**

****

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| Tài khoản | Tên đăng nhập và mật khẩu có quyền truy cập vào phần mềm được quy định ở bảng TaiKhoan trong CSDL. Người dùng sẽ nhập tên đăng nhập và mật khẩu vào các ô |
| Mật khẩu |  |
| Đăng nhập | Người dùng nhấn Đăng nhập và sẽ được vào giao diện chính của phần mềm nếu tài khoản và mật khẩu đúng và hợp lệ, ngược lại thông báo đăng nhập thất bại. |
| Thoát | Người dùng nhấn vào nút Thoát để rời khỏi phần mềm |

## **7.2. Form Quản lý**

****

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| MenuStrip (Quản lý) | Người dùng chọn quản lý sẽ hiện ra danh sách các mục như khách hàng, chi nhánh, nhân viên,... Người dùng chọn mục tương ứng với nhu cầu của mình, sau đó sẽ hiện lên giao diện quản lý tương ứng mà người dùng đã chọn |
| MenuStrip (Đăng xuất) | Người dùng nhấn Đăng xuất để trở về Form đăng nhập |
| Các button Menu, Nhân viên, Hóa đơn, Hóa đơn chi tiết, Khách hàng, Phiếu Nhập Hàng, Chi tiết nhập hàng, Tài khoản | Người dùng nhấn vào button tùy thuộc vào nhu cầu, sau đó sẽ hiện lên giao diện quản lý tương ứng mà người dùng đã chọn |

## **7.3. Form Menu**

**Chart

Description automatically generated with medium confidence**

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| Các text box(Mã nhân viên, tên nhân viên, số điện thoại, địa chỉ, CCCD, ngày sinh, giới tính) | Sau khi chọn chức năng thêm hoặc sửa, nhập dữ liệu vào vào các textbox |
| Thêm | Người dùng nhấn nút Thêm nếu muốn thêm một Menu mới , rồi nhập giá trị vào các text box |
| Sửa | Người dùng nhấn nút Sửa, sau đó nhập giá trị vào các textbox. |
| Xóa | Người dùng nhấn nút Xóa sau khi chọn nhân viên cần xóa ở datagrid view. Thông báo sẽ xuất hiện tương tự khi chọn chức năng xóa. |
| Trang chủ | Nhấn vào nút này sẽ trở về lại trang quản lý |
| Tìm kiếm | Người dùng chọn tiêu chí và nhập giá trị tương ứng vào textbox tìm kiếm, nếu dữ liệu trùng khớp thì ở datagrid view sẽ xuất hiện dữ liệu cần tìm |
| Resert | Khi nhấn nút này các textbox sẽ tự động trở lại trạng thái ban đầu, tức không có dữ liệu trên textbox. |

## **7.4. Form Hóa đơn**

**Table

Description automatically generated**

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| Các text box(Mã nhân viên, tên nhân viên, số điện thoại, địa chỉ, CCCD, ngày sinh, giới tính) | Sau khi chọn chức năng thêm hoặc sửa, nhập dữ liệu vào vào các textbox |
| Thêm | Người dùng nhấn nút Thêm nếu muốn thêm một hóa đơn mới , rồi nhập giá trị vào các text box |
| Sửa | Người dùng nhấn nút Sửa, sau đó nhập giá trị vào các textbox. Người dùng không thể sửa mã món. |
| Xóa | Người dùng nhấn nút Xóa sau khi chọn nhân viên cần xóa ở datagrid view. Thông báo sẽ xuất hiện tương tự khi chọn chức năng xóa. |
| Trang chủ | Nhấn vào nút này sẽ trở về lại trang quản lý |
| Tìm kiếm | Người dùng chọn tiêu chí và nhập giá trị tương ứng vào textbox tìm kiếm, nếu dữ liệu trùng khớp thì ở datagrid view sẽ xuất hiện dữ liệu cần tìm |
| Resert | Khi nhấn nút này các textbox sẽ tự động trở lại trạng thái ban đầu, tức không có dữ liệu trên textbox. |

## **7.5. Form Chi tiết hóa đơn**

**Table

Description automatically generated**

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| Các text box(Mã nhân viên, tên nhân viên, số điện thoại, địa chỉ, CCCD, ngày sinh, giới tính) | Sau khi chọn chức năng thêm hoặc sửa, nhập dữ liệu vào vào các textbox |
| Thêm | Người dùng nhấn nút Thêm nếu muốn thêm một chi tiết hóa đơn mới khi đã tạo 1 hóa đơn trống , rồi nhập giá trị vào các text box |
| Sửa | Người dùng nhấn nút Sửa, sau đó nhập giá trị vào các textbox. Người dùng không thể sửa mã hóa đơn. |
| Xóa | Người dùng nhấn nút Xóa sau khi chọn nhân viên cần xóa ở datagrid view. Thông báo sẽ xuất hiện tương tự khi chọn chức năng xóa. |
| Trang chủ | Nhấn vào nút này sẽ trở về lại trang quản lý |
| Tìm kiếm | Người dùng chọn tiêu chí và nhập giá trị tương ứng vào textbox tìm kiếm, nếu dữ liệu trùng khớp thì ở datagrid view sẽ xuất hiện dữ liệu cần tìm |
| Resert | Khi nhấn nút này các textbox sẽ tự động trở lại trạng thái ban đầu, tức không có dữ liệu trên textbox. |

## **7.6. Form Nhân viên**

**Table

Description automatically generated**

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| Các text box(Mã nhân viên, tên nhân viên, số điện thoại, địa chỉ, CCCD, ngày sinh, giới tính) | Sau khi chọn chức năng thêm hoặc sửa, nhập dữ liệu vào vào các textbox |
| Thêm | Người dùng nhấn nút Thêm nếu muốn thêm một nhân viên mới, rồi nhập giá trị vào các text box |
| Sửa | Người dùng nhấn nút Sửa, sau đó nhập giá trị vào các textbox. Người dùng không thể sửa mã nhân viên |
| Xóa | Người dùng nhấn nút Xóa sau khi chọn nhân viên cần xóa ở datagrid view. Thông báo sẽ xuất hiện tương tự khi chọn chức năng xóa. |
| Trang chủ | Nhấn vào nút này sẽ trở về lại trang quản lý |
| Tìm kiếm | Người dùng chọn tiêu chí và nhập giá trị tương ứng vào textbox tìm kiếm, nếu dữ liệu trùng khớp thì ở datagrid view sẽ xuất hiện dữ liệu cần tìm |
| Resert | Khi nhấn nút này các textbox sẽ tự động trở lại trạng thái ban đầu, tức không có dữ liệu trên textbox. |

## **7.7. Form Khách Hàng**

**Graphical user interface

Description automatically generated**

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| Các text box(Mã khách hàng, tên khách hàng, số điện thoại, địa chỉ, tìm kiếm) | Sau khi chọn chức năng thêm hoặc sửa, nhập dữ liệu vào vào các textbox |
| Thêm | Người dùng nhấn nút Thêm nếu muốn thêm một khách hàng mới, rồi nhập giá trị vào các text box |
| Sửa | Người dùng nhấn nút Sửa, sau đó nhập giá trị vào các textbox. Người dùng không thể sửa mã khách hàng |
| Xóa | Người dùng nhấn nút Xóa sau khi chọn khách hàng cần xóa ở datagrid view. Thông báo sẽ xuất hiện tương tự khi chọn chức năng xóa ở các bảng khác |
| Trang chủ | Nhấn vào nút này sẽ trở về lại trang quản lý |
| Tìm kiếm | Người dùng chọn tiêu chí và nhập giá trị tương ứng vào textbox tìm kiếm, nếu dữ liệu trùng khớp thì ở datagrid view sẽ xuất hiện dữ liệu cần tìm |
| Resert | Khi nhấn nút này các textbox sẽ tự động trở lại trạng thái ban đầu, tức không có dữ liệu trên textbox. |

## **7.8. Form Phiếu nhập hàng**

**Graphical user interface

Description automatically generated with low confidence**

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| Các text box(Mã nhân viên, tên nhân viên, số điện thoại, địa chỉ, CCCD, ngày sinh, giới tính) | Sau khi chọn chức năng thêm hoặc sửa, nhập dữ liệu vào vào các textbox |
| Thêm | Người dùng nhấn nút Thêm nếu muốn thêm một phiếu hàng mới , rồi nhập giá trị vào các text box |
| Sửa | Người dùng nhấn nút Sửa, sau đó nhập giá trị vào các textbox. Người dùng không thể sửa mã món. |
| Xóa | Người dùng nhấn nút Xóa sau khi chọn nhân viên cần xóa ở datagrid view. Thông báo sẽ xuất hiện tương tự khi chọn chức năng xóa. |
| Trang chủ | Nhấn vào nút này sẽ trở về lại trang quản lý |
| Tìm kiếm | Người dùng chọn tiêu chí và nhập giá trị tương ứng vào textbox tìm kiếm, nếu dữ liệu trùng khớp thì ở datagrid view sẽ xuất hiện dữ liệu cần tìm |
| Resert | Khi nhấn nút này các textbox sẽ tự động trở lại trạng thái ban đầu, tức không có dữ liệu trên textbox. |

## **7.9 Form Chi tiết nhập hàng**

**Table

Description automatically generated**

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| Các text box(Mã nhân viên, tên nhân viên, số điện thoại, địa chỉ, CCCD, ngày sinh, giới tính) | Sau khi chọn chức năng thêm hoặc sửa, nhập dữ liệu vào vào các textbox |
| Thêm | Người dùng nhấn nút Thêm nếu muốn thêm một chi tiết nhập hàng mới khi đã tạo 1 phiếu hàng trống, rồi nhập giá trị vào các text box |
| Sửa | Người dùng nhấn nút Sửa, sau đó nhập giá trị vào các textbox. Người dùng không thể sửa mã món. |
| Xóa | Người dùng nhấn nút Xóa sau khi chọn nhân viên cần xóa ở datagrid view. Thông báo sẽ xuất hiện tương tự khi chọn chức năng xóa. |
| Trang chủ | Nhấn vào nút này sẽ trở về lại trang quản lý |
| Tìm kiếm | Người dùng chọn tiêu chí và nhập giá trị tương ứng vào textbox tìm kiếm, nếu dữ liệu trùng khớp thì ở datagrid view sẽ xuất hiện dữ liệu cần tìm |
| Resert | Khi nhấn nút này các textbox sẽ tự động trở lại trạng thái ban đầu, tức không có dữ liệu trên textbox. |

## **7.10. Form Tài khoản**

**Graphical user interface

Description automatically generated**

|  |  |
| --- | --- |
| **Các thành phần** | **Chức năng** |
| Các textbox nhập dữ liệu(Username, pass,T\_type) | Nhập dữ liệu vào vào các ô để thực hiện các chức năng (Tìm, Thêm, Sửa, Xóa) |
| Thêm | Người dùng nhấn nút Thêm để tạo tài khoản mới |
| Sửa | Nhấn nút Sửa khi người dùng muốn sửa thông tin tài khoản, sau đó nhập đủ giá trị trên các text box.Người dùng chỉ có thể sửa pass và T\_type. |
| Xóa | Người dùng nhấn nút này để xóa tài khoản sau khi chọn tài khoản muốn xóa ở datagrid view. Sau đó nó sẽ hiện thông báo đã xóa. |
| Resert | Khi nhấn nút này các textbox sẽ tự động trở lại trạng thái ban đầu, tức không có dữ liệu trên textbox. |
| Trang chủ | Nhấn vào nút này sẽ trở về lại trang quản lý |
| Tìm kiếm | Người dùng chọn tiêu chí và nhập giá trị tương ứng vào textbox tìm kiếm, nếu dữ liệu trùng khớp thì ở datagrid view sẽ xuất hiện dữ liệu cần tìm |

# **8. Phương án giải quyết vấn đề dữ liệu lớn**

Vấn đề đặt ra: Giả sử lượng dữ liệu rất lớn, không đủ lưu trong một ổ đĩa.

Để giải quyết vấn đề dữ liệu lớn, nhóm đã chọn Cloud Cluster là cloud chứa dữ liệu. Nhóm sẽ tạo Database và các User, những thành viên trong nhóm sẽ có một tài khoản để đăng nhập, tài khoản sẽ được Read & Write.

**A screenshot of a computer

Description automatically generated**

Muốn lấy dữ liệu từ trên cloud, mỗi thành viên sẽ connect với tài khoản đã được tạo. Server name:  mssql-98375-0.cloudclusters.net,18006.

Lựa chọn SQL Server Authentication

Graphical user interface

Description automatically generated

# **9. Đề phòng phương án hệ thống bị tấn công bằng SQL Injection**

### 9.1. SQL Injection là gì?

SQL Injection được biết đến như một cách tấn công kho dữ liệu SQL vô cùng nguy hiểm. Những hậu quả nó để lại là vô cùng to lớn, với SQL Injection, hacker có thể truy cập một phần hoặc toàn bộ dữ liệu trong hệ thống.

Lỗi SQL Injection là một dạng tấn công thông qua những lỗ hổng trong bảo mật dữ liệu của một hệ thống. Bằng cách chèn các đoạn mã vào trong entry field, hacker sẽ tiến hành xâm nhập ứng dụng chứa dữ liệu của toàn bộ hệ thống. Các lệnh SQL độc hại ở đây có thể là đề xuất kết nối từ cơ sở dữ liệu cho hacker hoặc cấp phép truy cập cho những đối tượng không được phép.

### 9.2. Một số phương án phòng chống.

Để phòng ngừa SQL Injection, nhóm lựa chọn một số phương án sau:

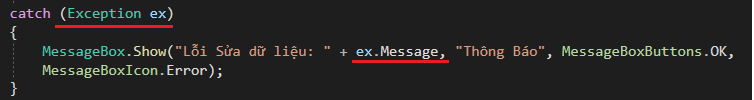
* Không sử dụng các câu lệnh cộng chuỗi để tạo SQL, thay vào đó là sử dụng thủ tục và Parameter. Như vậy thì các tham số đầu vào sẽ được kiểm soát, nếu dữ liệu truyền vào không hợp pháp, SQL Engine sẽ tự động báo lỗi, ta không cần dùng code để check.

Text

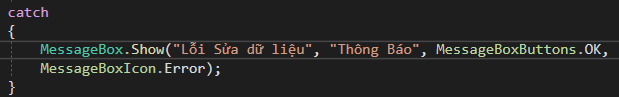
Description automatically generated

* Không hiển thị exception, message lỗi: Hacker dựa vào message lỗi để tìm ra cấu trúc database. Khi có lỗi, ta chỉ hiện thông báo lỗi chứ đừng hiển thị đầy đủ thông tin về lỗi, tránh hacker lợi dụng.

Không được hiện đầy đủ lỗi :



Chỉ hiện hông báo có lỗi như sau:



* Phân quyền rõ ràng trong DB: Nếu chỉ truy cập dữ liệu từ một số bảng, hãy tạo một account trong DB, gán quyền truy cập cho account đó chứ đừng dùng account root hay sa. Lúc này, dù hacker có inject được SQL cũng không thể đọc dữ liệu từ các bảng chính, sửa hay xóa dữ liệu.

Backup dữ liệu thường xuyên: Dữ liệu phải thường xuyên được backup để nếu có bị hacker xóa thì ta vẫn có thể khôi phục được

Link github: [santoryu31/Nhom\_9\_QTCSDL (github.com)](https://github.com/santoryu31/Nhom_9_QTCSDL)