

Requirement & Design Specification

**Online Course Management System (OCMS)**

**Version: 1.0**

– Hanoi, September 2024 –

# Record of Changes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | A\* M, D | In charge | Change Description |
| V1.0 | 18/9/2024 | A | manhpthe172481 | Database design |
| V2.0 | 19/9/2024 | A | manhpthe172481 | 2.1 Actor  2.2.1 UC for login |
| V2.0 | 25/9/2024 | A |  |  |
|  |  | A |  |  |
|  |  | A |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

\*A - Added M - Modified D - Deleted

Contents

[Record of Changes 2](#_Toc178395340)

[I. Overview 4](#_Toc178395341)

[1. System Context 4](#_Toc178395342)

[2. User Requirements 4](#_Toc178395343)

[2.1 Actors 4](#_Toc178395344)

[2.2 Diagrams 5](#_Toc178395345)

[2.3 Descriptions 6](#_Toc178395346)

[II. Functional Requirements 6](#_Toc178395347)

[1. <<Feature Name1>> 6](#_Toc178395348)

[1.1 <<Screen/Function Name1>> 6](#_Toc178395349)

[1.2 User Login 6](#_Toc178395350)

[1.3 … 7](#_Toc178395351)

[2. System Administration 7](#_Toc178395352)

[2.1 System Settings 7](#_Toc178395353)

[2.2 … 8](#_Toc178395354)

[3. … 8](#_Toc178395355)

[III. System Design 8](#_Toc178395356)

[1. Database Design 8](#_Toc178395357)

[1.1 Database Schema 9](#_Toc178395358)

[1.2 Table Descriptions 9](#_Toc178395359)

[2. Code Packages 9](#_Toc178395360)

[2.1 Package Diagram 10](#_Toc178395361)

[2.2 Package Descriptions 10](#_Toc178395362)

# I. Overview

## 1. System Context

The **Online Course Management System (OCMS)** is designed to help universities manage courses, student enrolment, and academic progress. It allows students to enrol in courses, access course materials, and track their progress. Instructors can manage course content, assignments, and assessments, while administrators oversee the overall course offerings and user management. The OCMS interacts with several external entities, including students, instructors, administrators, a payment system, and notification services like email or SMS. Students enrol in courses, submit assignments, and receive course materials and grades. Instructors create courses, provide learning materials, and grade students. Administrators manage user accounts, monitor enrolment, and generate system reports. The payment system handles transactions related to course enrolment, and notification services send important alerts to users regarding updates or deadlines. These interactions ensure a seamless flow of information between all parties involved, supporting the entire lifecycle of course management.

## 2. User Requirements

### 2.1 Actors

|  |  |  |
| --- | --- | --- |
| **#** | **Actor** | **Description** |
| 1 | Student | The student actor represents all users enrolled in the system to access course materials, enroll in courses, submit assignments, and track academic progress. They provide input data such as enrolment requests, assignment submissions, and receive outputs like course materials, grades, and notifications. |
| 2 | Instructor | The instructor actor represents all users responsible for creating and managing course content, grading assignments, and interacting with students. Instructors input course materials and grades into the system, and the system returns student submissions and grades for review. |
| 3 | Administrator | The administrator actor oversees system management, including user account administration, course catalogue management, and enrolment monitoring. Administrators provide input for system configurations and user management, receiving reports and system notifications in return. |

### 2.2 Diagrams

#### 2.2.1 UCs for Student

A diagram of a network

Description automatically generated

#### 2.2.2 UCs for Administrator

A diagram of a network

Description automatically generated with medium confidence

### 2.3 Descriptions

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Use Case** | **Actors** | **Use Case Description** |
| 01 | Log in | Student, Admin | Actor provides valid credentials (username and password) to authenticate and gain access to the system. |
| 02 | Login with Google | Student, Admin | Actor authorize the system to access to resource in Google via OAuth2 |
| 03 | Log out | Student, Admin | Actor terminates the session, effectively logging out of the system. |
| 04 | Forgot password | Student, Admin | Actor provides their email or username to request a password reset link, which will be sent to their registered email address. |
| 05 | Register | Student | Student provides required information (name, email, password, etc.) to create a new account in the system. |
| 06 | View Profile | Student, Admin | Actor views their personal profile information, including name, contact details, and any other relevant account data. |
| 07 | Edit Profile | Student, Admin | Actor updates their personal profile information, such as contact details or preferences. |
| 08 | Change password | Student, Admin | Actor updates their password by providing the current password and setting a new one. |
| 09 | View accounts | Admin | Admin views a list of all user accounts registered in the system, including students and other admins. |
| 10 | Deactivate account | Admin | Admin deactivates a user account, which prevents the user from logging into the system or accessing any services. |
| 11 | Edit account | Admin | Admin modifies account details for a specific user, such as updating roles, permissions, or personal information. |

# II. Functional Requirements

## 1. Authentication

### 1.1 <<Screen/Function Name1>>

### 1.2 User Login

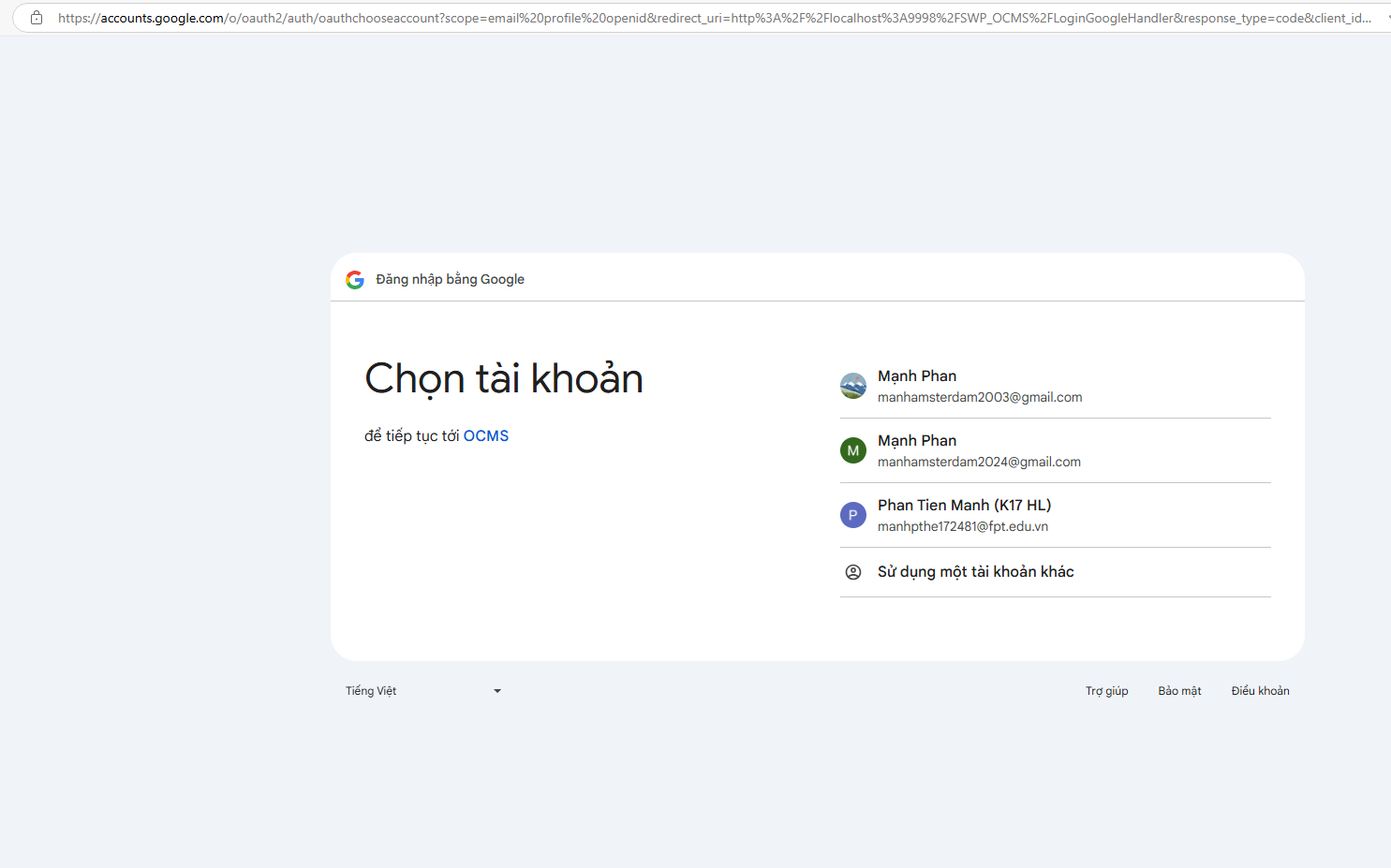
This is the Login screen for the Online Course Management System (OCMS). The purpose of this screen is to authenticate users (Students, Admins, or Instructors) and allow them to access their respective dashboards. Users can either log in using their email and password or opt for a Google login for easier access

Screen Specifications

1. **Field Initializations**:
   * **Email**: Empty by default, expects the user to input a valid email address.
   * **Password**: Empty by default, expects the user to input their password.
   * **Remember Me**: Unchecked by default. If checked, the system will store the session and automatically log the user in the next time they visit.
2. **Button Behaviors**:
   * **Continue with Google**: Redirects to Google OAuth for authentication. If successful, the user is redirected back to their dashboard.
   * **Sign In**: Verifies the email and password entered. If valid, the user is directed to their respective dashboard. If invalid, an error message is displayed.
   * **Forgot Password**: Redirects the user to a password reset form.
   * **Sign Up**: Redirects the user to the account registration page.
3. **Business Rules**:
   * Users must provide valid credentials (correct email format, non-empty password) to log in.
   * The system should handle failed login attempts with appropriate error messages (e.g., "Invalid email or password").
   * If the user logs in successfully, the system should redirect to the appropriate dashboard based on their role (Student, Admin, or Instructor).
4. **Normal Flow**:
   * User enters valid **email** and **password**.
   * Clicks **Sign In**.
   * The system authenticates the user and redirects to their dashboard.
5. **Alternative Flow**:
   * **Forgot Password Flow**: If the user clicks "Forgot Password," they are taken to a screen where they can request a password reset link to be sent to their email.
   * **Google Login Flow**: If the user chooses **Google login**, they are redirected to Google OAuth, where they must approve access. Upon successful authentication, they are directed back to their dashboard.

A screenshot of a login form

Description automatically generated



### 1.3 Log out

This screen represents the header for the user after they have logged into the Online Course Management System (OCMS). Its primary function is to give the user access to navigation options and to allow them to log out of the system when desired. The user can click on the **Log out** button to safely end their session and return to the login page or homepage.

Screen Specifications

1. **Field Initializations**:
   * **Navigation links**: All links (Home, Courses, Dashboard) are visible and initialized based on the user's login status. After login, they are fully accessible.
   * **Favorites and Cart icons**: Both icons are initialized with a count of items (number of favorites and items in the cart).
   * **Log out button**: This button is visible only when the user is logged in. If clicked, it logs the user out and redirects them to the login or home page.
2. **Button Behaviors**:
   * **Log out button**: When clicked, it terminates the session, clears user session data, and redirects the user to the login screen. The button is only visible when the user is authenticated.
3. **Business Rules**:
   * Users must be logged in to access this screen (navigation options and log out button).
   * Clicking the **Log out** button will:
     + Invalidate the user’s session.
     + Clear any session-based data (e.g., authentication tokens, cached personal information).
     + Redirect the user to the homepage or login screen depending on the system configuration.
4. **Normal Flow**:
   * User clicks on the **Log out** button.
   * The system logs the user out, invalidates the session, and redirects the user to the login page.
5. **Alternative Flow**:
   * If the user navigates away from the screen without logging out, their session will remain active until they manually log out or their session times out.



### 1.4 Forgot password

The **Forgot Password** functionality is a multi-step process that allows users to reset their password in case they have forgotten it. The process is divided into three key screens:

1. **Forgot Password Screen**: This screen prompts the user to input their email address to receive a password reset link.
2. **Enter OTP Code Screen**: After receiving the OTP via email, the user must input the correct OTP code to proceed.
3. **Reset Password Screen**: This screen allows the user to enter a new password and confirm it to reset their account.

Screen Specifications

1. **Forgot Password Screen**
   * **Field Initializations**:
     + **Email Address Field**: Empty by default. The user must input a valid registered email address.
     + **Reset Password Button**: Enabled when a valid email is entered.
   * **Business Rules**:
     + The email field must be validated (check for valid format, and that the email is registered in the system).
     + If the email is valid, the system sends a password reset link or OTP code to the provided email address.
     + If the email is not found, an error message appears prompting the user to enter a valid email.
   * **Normal Flow**:
     + User enters their email and clicks **Reset Password**.
     + The system sends a password reset email with an OTP or link to the user’s email.
   * **Alternative Flow**:
     + If the email address is invalid or not found in the system, an error message will display ("Invalid email address").
2. **Enter OTP Code Screen**
   * **Field Initializations**:
     + **OTP Code Field**: Empty by default, expects the user to enter the OTP sent to their email.
     + **Verify OTP Button**: Enabled once an OTP is entered.
   * **Business Rules**:
     + The OTP code is validated against the system's records. If the code matches, the user proceeds to reset their password.
     + If the OTP is incorrect, the user can try again or request a new OTP code via the **Resend OTP** link.
   * **Normal Flow**:
     + User enters the OTP and clicks **Verify OTP**.
     + The system verifies the OTP, and if valid, it redirects the user to the password reset screen.
   * **Alternative Flow**:
     + If the OTP is incorrect, the user is prompted with an error message ("Invalid OTP").
     + The user can request a new OTP using the **Resend OTP** link.
3. **Reset Password Screen**
   * **Field Initializations**:
     + **New Password Field**: Empty by default, expects the user to enter a new password.
     + **Confirm New Password Field**: Empty by default, requires confirmation of the password entered in the first field.
     + **Reset Password Button**: Enabled when both fields are filled, and the passwords match.
   * **Business Rules**:
     + Passwords must meet the system’s security requirements (minimum length, inclusion of special characters, etc.).
     + The two password fields must match to proceed.
   * **Normal Flow**:
     + The user enters a new password and confirms it by re-entering it in the second field.
     + If the passwords match and meet the system requirements, the user clicks **Reset Password**.
     + The system updates the user’s password and redirects them to the login page.
   * **Alternative Flow**:
     + If the passwords do not match, an error message appears, prompting the user to correct the input ("Passwords do not match").
     + If the password does not meet security criteria, an error message suggests a stronger password.

A screenshot of a login page

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a login screen

Description automatically generated

### 1.5 Register

The **Register screen** in the Online Course Management System (OCMS) is designed for new users to create an account. This screen allows users to either register by providing an email and password or use their **Google** account for quicker registration. The registration process is secured by email verification, using an **OTP** (One-Time Password) sent to the user’s email. The process is divided into two key screens:

1. **Create Account**: Users enter their email, password, and confirm the password.
2. **Enter OTP Code**: Users input the OTP sent to their email to verify the account.

Screen Specifications

1. **Create Your Account Screen**
   * **Field Initializations**:
     + **Email Field**: Empty by default. Expects a valid email format.
     + **Password Field**: Empty by default. Requires the user to input a password that adheres to security standards.
     + **Confirm Password Field**: Empty by default. The user must re-enter the same password for confirmation.
   * **Business Rules**:
     + **Google Sign-In Option**: Allows users to register using their Google account. The system retrieves necessary information like email and bypasses manual input.
     + **Email Validation**: The email field must contain a valid email format (e.g., user@example.com). If invalid, the system displays an error.
     + **Password Validation**: The password must meet the system's security requirements, such as minimum length and inclusion of alphanumeric or special characters.
     + **Password Matching**: The password and confirm password fields must match. If they do not, an error message is shown ("Passwords do not match").
     + After a successful sign-up attempt, the system sends an OTP code to the user’s email to verify the account.
   * **Normal Flow**:
     + User fills in the email, password, and confirms the password.
     + Clicks **Sign Up**.
     + The system validates the fields, registers the account, and sends an OTP code to the user's email.
   * **Alternative Flow**:
     + If any field is invalid (e.g., incorrect email format, weak password, or mismatching passwords), the user is prompted with error messages and needs to correct the input.
2. **Enter OTP Code Screen**
   * **Field Initializations**:
     + **OTP Code Field**: Empty by default. Expects the user to input the OTP received via email.
     + **Verify OTP Button**: Enabled once an OTP is entered.
   * **Business Rules**:
     + The OTP must match the code sent to the user’s email. If the user enters the wrong code, an error message is displayed ("Invalid OTP").
     + If the OTP is not received, the user can request another OTP via the **Resend OTP** link.
     + After verifying the OTP, the account is successfully created, and the user is redirected to the login or dashboard screen.
   * **Normal Flow**:
     + User enters the OTP code and clicks **Verify OTP**.
     + The system checks if the OTP matches the one sent via email. If valid, the account is verified.
   * **Alternative Flow**:
     + If the OTP is invalid or expired, the user is prompted to either try again or request a new code via **Resend OTP**.

A screenshot of a login form

Description automatically generated

A screenshot of a computer

Description automatically generated

### 1.6 View Profile

The **View Profile screen** in the Online Course Management System (OCMS) allows logged-in users to view and manage their personal information, including email, role, gender, and last login details. This screen is accessible after the user logs into the system and clicks on the **Dashboard** button in the header. The screen gives users an overview of their profile details and provides an option to update their information.

**Screen Specifications**

1. **Field Initializations**:
   * **Email Field**: Pre-filled with the email address of the user based on the data stored in the system.
   * **Role Field**: Displays the user’s role (e.g., Student, Admin, Instructor). This field is usually non-editable as it’s defined by system roles.
   * **Gender Field**: Pre-selected based on the user’s previous selection or profile settings.
   * **Last Login Field**: Displays the timestamp of the last login for the user.
2. **Update Profile Button**:
   * The **Update Profile** button allows the user to modify their profile information, such as gender or other details (if applicable), and save the changes. Once clicked, the system validates the changes and updates the user profile accordingly.
3. **Business Rules**:
   * **Login Requirement**: Users must be logged in to access the **Dashboard** and **Profile** page. If a user tries to access this page without being logged in, they will be redirected to the login page.
   * **Data Validation**: When updating profile details, the system checks for valid input (e.g., valid email format). If validation fails, an error message will prompt the user to correct their input.
   * **Update Profile**: Only certain fields like gender and contact information may be editable, while fields like email and role may be locked based on system rules.
4. **Normal Flow**:
   * The user logs into the system using their credentials.
   * After logging in, the user clicks on the **Dashboard** link in the header.
   * The user is directed to the **Dashboard**, where they click on the **My Profile** option in the sidebar.
   * The **Profile screen** is loaded, displaying the user’s profile information.
   * The user can view their details and update fields where applicable.
   * If the user modifies any data, they click **Update Profile** to save the changes.
5. **Alternative Flow**:
   * If the user is not logged in and attempts to access the profile page, they are redirected to the login page.
   * If the user tries to submit invalid data (e.g., incorrect email format), the system will display an error message and prompt the user to correct the information before submitting again.

This **View Profile screen** is a crucial part of the OCMS that allows users to manage and review their personal data securely after authentication.

A screenshot of a computer

Description automatically generated

### 1.7 Edit Profile

The **Edit Profile screen** in the Online Course Management System (OCMS) allows users to view and modify their profile information. This screen is accessed after the user has logged in, navigated to the **Dashboard**, and clicked on the **My Profile** option. The user can update certain fields like their gender or other personal details and save changes by clicking the **Update Profile** button.

**Screen Specifications**

1. **Field Initializations**:
   * **Email Field**: Pre-filled with the user's registered email address. This field is typically non-editable for security reasons.
   * **Role Field**: Displays the user’s role (e.g., Student, Admin, Instructor). This field is non-editable as the role is assigned by the system.
   * **Gender Field**: Pre-selected based on the user’s current profile information but can be updated. Users can select their gender from a dropdown list.
   * **Last Login Field**: Displays the timestamp of the user's last login. This field is non-editable and only for informational purposes.
2. **Update Profile Button**:
   * When clicked, this button saves the changes made to the editable fields. Once submitted, the system checks for any validation errors and updates the user’s profile if all inputs are valid.
3. **Business Rules**:
   * **Validation**: Before saving any changes, the system ensures that all fields follow the correct format (e.g., valid email, selection from dropdown lists). Although the email cannot be changed on this screen, all other fields must be validated.
   * **Editable Fields**: Only certain fields like **gender** are editable. Fields like **email** and **role** are locked and cannot be changed by the user.
   * **Successful Update**: Upon clicking **Update Profile**, if validation is successful, the profile changes are saved, and the user may receive a confirmation message.
4. **Normal Flow**:
   * The user logs in and navigates to the **Dashboard**.
   * The user selects **My Profile** from the sidebar, landing on the **Edit Profile** screen.
   * The user makes changes to editable fields (e.g., gender) and clicks **Update Profile**.
   * The system validates the changes and saves the updated information, reflecting the changes on the profile page.
5. **Alternative Flow**:
   * If the user enters invalid data (e.g., selecting invalid options), the system will prompt an error message requesting the user to correct the input before proceeding.
   * If the user attempts to modify non-editable fields like **email** or **role**, the system will prevent the changes from being made.

The **Edit Profile screen** ensures users can manage and update their personal information securely, while ensuring that critical fields such as email and role remain protected from user changes.

A screenshot of a computer

Description automatically generated

### 1.8 Change password

The **Change Password screen** in the Online Course Management System (OCMS) allows authenticated users to update their account password. This screen is accessed from the user’s **Dashboard**, specifically by selecting the **Change Password** option from the sidebar. The purpose of this screen is to ensure users can securely modify their password by providing their current password and a new password, which is verified through a confirmation field.

**Screen Specifications**

1. **Field Initializations**:
   * **Current Password Field**: This field is empty by default and requires the user to input their existing password for verification.
   * **New Password Field**: Empty by default, expects the user to enter a new password.
   * **Confirm New Password Field**: Empty by default, expects the user to re-enter the new password for confirmation.
2. **Change Password Button**:
   * This button is disabled until all fields are filled. Once the fields are completed with valid data, the button becomes active, allowing the user to submit the password change request.
3. **Business Rules**:
   * **Current Password Validation**: The system checks if the entered current password matches the user’s existing password stored in the system.
   * **New Password Validation**: The new password must meet security criteria such as minimum length, inclusion of numbers or special characters, etc.
   * **Password Confirmation**: The system checks if the **New Password** and **Confirm New Password** fields match. If they do not match, an error message is displayed, prompting the user to re-enter the passwords.
   * **Password Reuse Prevention**: The system may have a rule that prevents the user from using the same password as their previous one.
4. **Normal Flow**:
   * The user logs in, navigates to the **Dashboard**, and selects the **Change Password** option from the sidebar.
   * The user enters their current password in the first field, followed by the new password in the second field, and confirms the new password in the third field.
   * The user clicks **Change Password**.
   * The system validates the current password and ensures the new password follows the security rules and matches the confirmation field.
   * If all validations pass, the system updates the password and displays a success message.
5. **Alternative Flow**:
   * If the **Current Password** is incorrect, the system displays an error message ("Incorrect current password"), and the user must try again.
   * If the **New Password** and **Confirm New Password** do not match, the system prompts the user to correct the input with an error message ("Passwords do not match").
   * If the new password does not meet security requirements, an error message is shown advising the user to follow the password guidelines (e.g., minimum length, special characters).

The **Change Password screen** ensures that users can securely update their passwords while adhering to security standards. The three-step process of entering the current password, new password, and confirming the new password ensures the integrity of the password update operation.

A screenshot of a computer

Description automatically generated

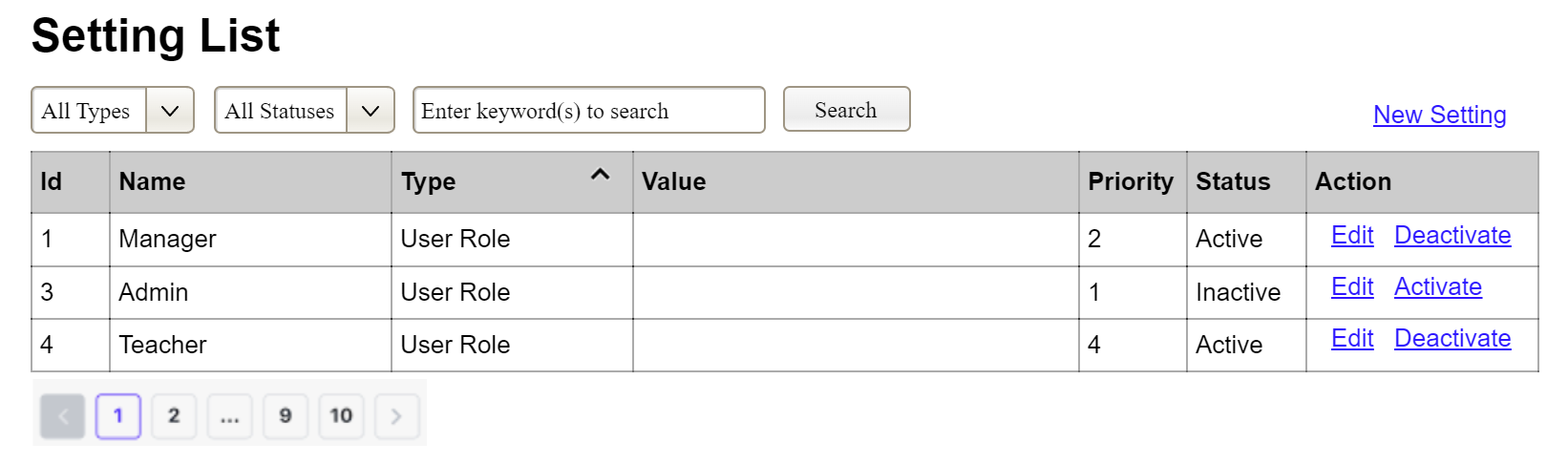
## 2. System Administration

### 2.1 System Settings

#### 2.1.1 Setting List

After clicking the System Configurations link on the NavBar (sider) menu, this page is shown.

This is for the administrator to view the list of current system settings. On this page, s/he can also activate or deactivate (change status) of a specific setting.



(2)

(3)

(1)

(1) Setting Type:

* Initialized with all the active setting types filled in,
* Allow user to filter the setting list by a specific setting type
* Default value is “All Types”, allowing user to see the settings at all types

(2) Setting Status:

* Initialized with two values Active and Inactive filled in
* Allow user to filter the setting list by a specific status (Active or Inactive)
* Default value is “All Types”, allowing user to see the settings at all statuses

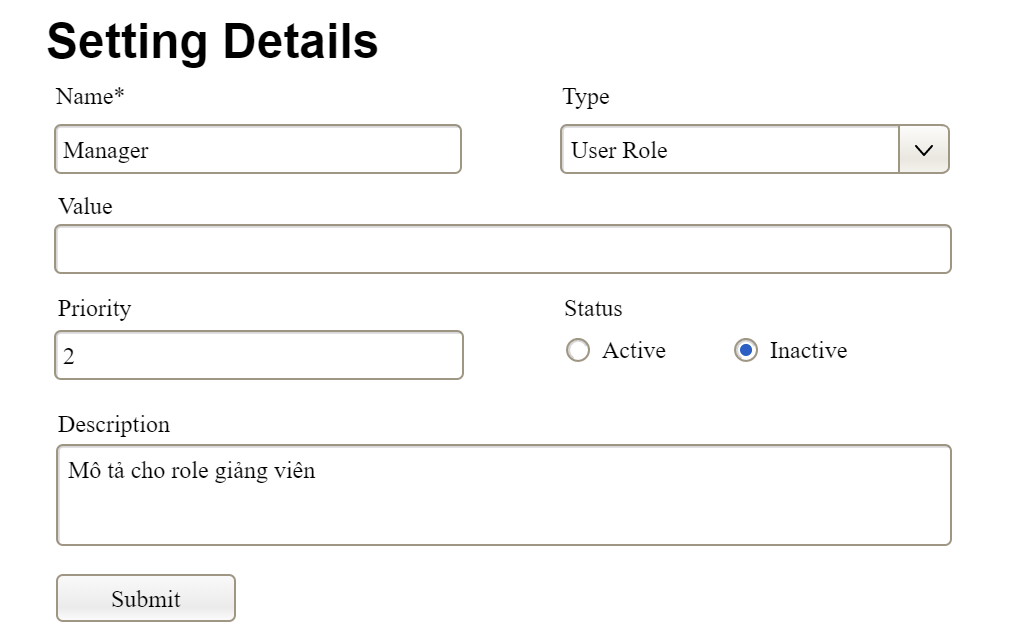
(3) The change-status action is Activate or Deactivate depending on the current status of the relevant setting (Inactive or Active, respectively). The user needs to confirm the status changing via a modal confirmation message before getting that done.

…

#### 2.1.2 Setting Details

This page is shown after the user click the New Setting link or the Edit link in the [Setting List](#_2.1.1_Setting_List) page

This is for the administrator to add new or view/update an existing system setting



…

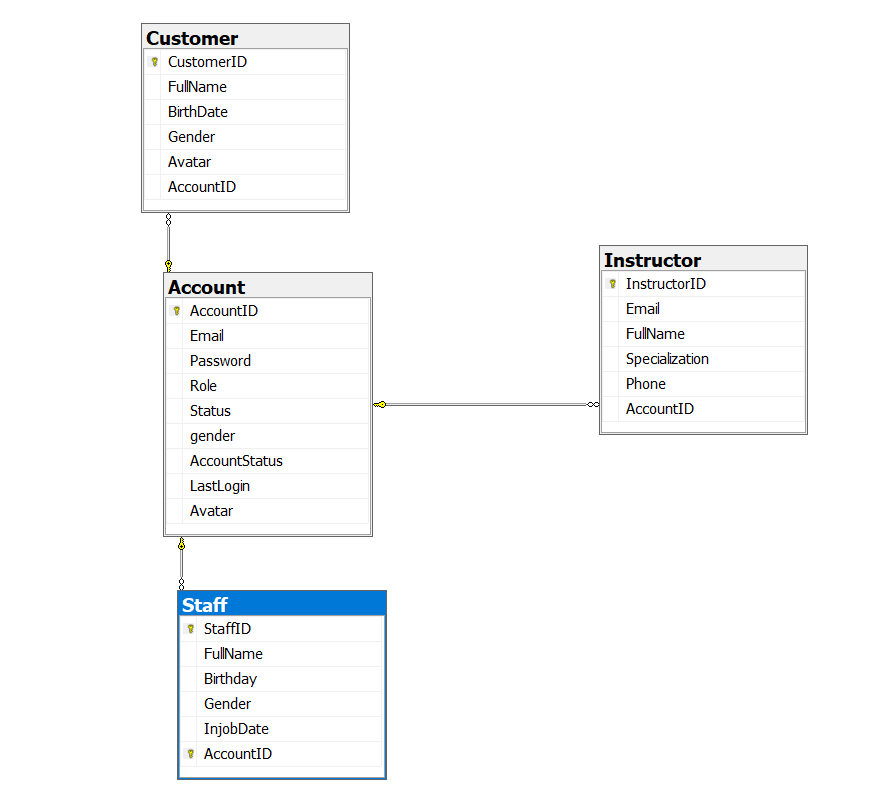
### 2.2 …

## 3. …

# III. System Design

## 1. Database Design

### 1.1 Database Schema



### 1.2 Table Descriptions

|  |  |  |
| --- | --- | --- |
| **No** | **Table** | **Description** |
| *01* | *Account* | [AccountID] [int] IDENTITY(1,1) NOT NULL,  [Email] [nvarchar](100) NULL,  [Password] [nvarchar](255) NULL,  [Role] [nvarchar](50) NULL,  [Status] [nvarchar](20) NULL,  [gender] [bit] NULL,  [AccountStatus] [nvarchar](20) NULL,  [LastLogin] [datetime] NULL,  [Avatar] [nvarchar](max) NULL, |
| *02* | *Customer* | [CustomerID] [int] NOT NULL,  [FullName] [nvarchar](100) NULL,  [BirthDate] [date] NULL,  [Gender] [nvarchar](10) NULL,  [Avatar] [varbinary](max) NULL,  [AccountID] [int] NULL, |
| *03* | *Instructor* | [InstructorID] [int] NOT NULL,  [Email] [nvarchar](100) NULL,  [FullName] [nvarchar](100) NULL,  [Specialization] [nvarchar](100) NULL,  [Phone] [nvarchar](20) NULL,  [AccountID] [int] NULL, |
| *04* | *Staff* | [StaffID] [int] NOT NULL,  [FullName] [nvarchar](100) NULL,  [Birthday] [date] NULL,  [Gender] [nvarchar](10) NULL,  [InjobDate] [date] NULL,  [AccountID] [int] NOT NULL, |

## 2. Code Packages

### 2.1 Package Diagram



### 2.2 Package Descriptions

|  |  |  |
| --- | --- | --- |
| **No** | **Package** | **Description** |
| *01* | *member\_authority* | *<Description of the package: purpose, contents,..>* |
| *02* | *registration* | *<Description of the package: purpose, contents,..>* |
| *03* | *…* |  |