The system shall enable users (Passengers) to initiate the creation of new accounts.

UC Name	*User Account Creation* *UC-201*
Summary	*Enabling passengers to create new accounts within the system.*
Dependency	*None*
Actors	Primary Actor: User (Passenger) Secondary Actor: System
Preconditions	*1.The user attempts to sign up using personal information.* *2.The user's unique account identifiers (email) do not match with another user's in the system.* *3.The user agrees to the terms and conditions of service before proceeding with the sign-up process.* *4. The user provides all required information fields (such as name, email, password) during the sign-up attempt.*
Description of the Main Sequence	*Step 1: The user navigates to the sign-up page on the system.* *Step 2: The user fills in the required personal information such as name, email address, and password.* *Step 3: The system validates the entered information to ensure all required fields are filled correctly.* *Step 4: The system checks if the provided email address is unique and not already associated with an existing account.* *Step 5: If the email address is unique, the system sends a verification email to the provided address.* *Step 6: The user receives the verification email and clicks on the verification link to confirm their email address.* *Step 7: Upon email verification, the system creates a new account for the user.* *Step 8: The user receives a confirmation message indicating successful account creation.* *Step 9: The user can now log in to the system using their email address and password.*
Description of the Alternative Sequence	**Alternative Sequence 1**: If the email address provided is already associated with an existing account, the system prompts the user to choose a different email address or attempt to recover their existing account.

	Alternative Sequence 2: If any errors occur during the sign-up process, such as invalid information or technical issues, the system provides appropriate error messages and prompts the user to correct the issues and try again.
Non functional requirements	**Security**: The security requirement for the sign-up process ensures the protection of user accounts and sensitive information from unauthorized access and potential breaches. **Performance**: The authentication process is expected to conclude within a specified duration of seconds. **Scalability**: The authentication database system should be capable of handling a large number of accounts.
Postconditions	● If account creation is successful, user should be able to login with their registered information. ● In case account creation fails, user shall not be able to login.

The system shall provide users (Passengers) with the ability to securely authenticate and access their accounts.

UC Name	*User Account Creation* *UC-202*
Summary	*Enabling passengers to securely access their accounts within the system.*
Dependency	*User Account Creation (UC-201)*
Actors	Primary Actor: User (Passenger) Secondary Actor: System
Preconditions	*1.The user has already created an account with the system.* *2.The user possesses valid login credentials, including a registered email address and password.* *3.The user has agreed to the terms and conditions of service before attempting to log in.* *4.The system is operational and accessible for user login.*
Description of the Main	*Step 1: The user enters their credentials to log in to the system.*

Sequence	*Step 2: The system verifies the provided credentials against the stored user data.* *Step 3: If the credentials match an existing user account, the system grants access to the user.*
Description of the Alternative Sequence	**Alternative Sequence 1**: If the credentials do not match or are invalid, the system denies access and prompts the user to try again or reset their password. **Alternative Sequence 2**: If any errors occur during the log-in process, such as invalid information or technical issues, the system provides appropriate error messages and prompts the user to correct the issues and try again.
Non functional requirements	**Security**: The security requirement for the login process ensures the protection of user accounts and sensitive information from unauthorized access and potential breaches. **Performance**: The authentication process is expected to conclude within a specified duration of seconds. **Scalability**: The authentication database system should be capable of handling a large number of accounts.
Postconditions	● 1. If the user's credentials are validated successfully, the user gains access to their account. ● 2. Upon successful login, the system may redirect the user to their account dashboard or another designated landing page. ● 3. If the user's credentials are invalid, the system denies access and provides appropriate error messages. ● 4. After a specified number of unsuccessful login attempts, the system may lock the user's account for security purposes. ● 5. The system logs the login activity, recording successful and unsuccessful login attempts for security auditing purposes.

The system shall grant administrators the capability to create new specialized permission accounts for privileged users.

UC Name	*Admin Account Creation* *UC-203*
Summary	*Enabling administrators to create accounts for privileged users.*
Dependency	*None*
Actors	Primary Actor: User (Admin) Secondary Actor: System
Preconditions	*1. The administrator has appropriate access privileges and permissions to create new accounts.* *2. The administrator is logged into the system.* *3. The system is operational and accessible.* *4. The administrator possesses all necessary information required to create the new accounts, including user details and assigned permissions.*
Description of the Main Sequence	*Step 1: The administrator accesses the account management section of the system.* *Step 2: The administrator fills in the required details for the new account, including username, email, and any additional information.* *Step 3: The administrator selects or defines the special permissions for the new account.* *Step 4: The system validates the entered information to ensure accuracy and completeness.* *Step 5: Upon successful validation, the administrator confirms the creation of the new account.* *Step 6: The system generates a confirmation message, indicating that the new account has been successfully created.* *Step 7: If applicable, the system sends a notification to the newly created account, providing login credentials and instructions.* *Step 8: The system logs the creation of the new account for auditing purposes.* *Step 9: The administrator is returned to the main interface or account management section for further actions.*
Description of the Alternative Sequence	**Alternative Sequence 1**: If during the account creation process, the system encounters a critical error such as database connectivity issues or server malfunction, it halts

	the account creation process, displays an error message informing the administrator of the technical issue, and advises them to attempt account creation again later or contact technical support for assistance.
Non functional requirements	-Reliability: The system should maintain consistent availability, minimizing downtime to ensure users can reliably access account creation and management functionalities. -Usability: The account creation interface should be intuitive and user-friendly, guiding administrators through the process with clear instructions and minimal complexity. -Scalability: The authentication database system should be capable of handling a large number of accounts. - Performance: The authentication process is expected to conclude within a specified duration of seconds. -Security: The security requirement for the sign up process ensures the protection of user accounts and sensitive information from unauthorized access and potential breaches.
Postconditions	1. The newly created account is added to the system's user database, allowing the administrator to manage its permissions and access rights. 2. The system generates a confirmation message, notifying the administrator of the successful account creation. 3. If applicable, the system sends a notification to the newly created account, providing login credentials and instructions on accessing the system. 4. The creation event is logged in the system's audit trail, recording details such as the administrator responsible, timestamp, and any relevant metadata for auditing purposes. 5. The administrator is returned to the main interface or account management section, ready for further actions or tasks.

The system shall grant administrators the capability to delete accounts from the system.

UC Name	*Admin Account Deletion* *UC-204*
Summary	*Enabling administrators to delete accounts for privileged users.*
Dependency	*None*
Actors	Primary Actor: User (Admin) Secondary Actor: System
Preconditions	*1. The administrator has appropriate access privileges and permissions to delete accounts.* *2. The administrator is logged into the system.* *3. The system is operational and accessible.* *4. The administrator possesses all necessary information required to identify the account to be deleted.*
Description of the Main Sequence	*Step 1: The administrator accesses the account management section of the system.* *Step 2: The administrator navigates to the list of user accounts and selects the account to be deleted.* *Step 3: The system prompts the administrator to confirm the deletion action.* *Step 4: The administrator confirms the deletion of the selected account.* *Step 5: The system removes the selected account from the user database.* *Step 6: The system generates a confirmation message, indicating that the account has been successfully deleted.* *Step 7: The deletion event is logged in the system's audit trail, recording details such as the administrator responsible, timestamp, and any relevant metadata for auditing purposes.* *Step 8: The administrator is returned to the main interface or account management section for further actions.*
Description of the Alternative Sequence	**Alternative Sequence 1**: If during the account deletion process, the system encounters a critical error such as database connectivity issues or server malfunction, it halts the account deletion

	process, displays an error message informing the administrator of the technical issue, and advises them to attempt account deletion again later or contact technical support for assistance.
Non functional requirements	• Usability: The account deletion interface should be intuitive and user-friendly, guiding administrators through the process with clear instructions and minimal complexity. • Performance: The account deletion process is expected to conclude within a specified duration of seconds. • Security: The security requirement for the account deletion process ensures that only authorized administrators can delete accounts, preventing unauthorized access to user data.
Postconditions	1. The selected account is successfully removed from the system's user database. 2. The system generates a confirmation message, notifying the administrator of the successful account deletion. 3.The administrator is returned to the main interface or account management section for further actions.

The system shall grant administrators the capability to reset the password of accounts.

UC Name	*Admin Password Reset* *UC-205*
Summary	*Enabling administrators to reset passwords for user accounts.*
Dependency	*User Account Creation (UC-201), Admin Account Creation (UC-203)*
Actors	Primary Actor: User (Admin) Secondary Actor: System

Preconditions	1. *The administrator has appropriate access privileges and permissions to reset passwords.* 2. *The administrator is logged into the system.* 3. *The system is operational and accessible.* 4. *The administrator possesses all necessary information required to identify the account for which the password needs to be reset.*
Description of the Main Sequence	*Step 1: The administrator accesses the account management section of the system.* *Step 2: The administrator navigates to the list of user accounts and selects the account for which the password needs to be reset.* *Step 3: The system prompts the administrator to enter a new password for the selected account.* *Step 4: The administrator enters the new password.* *Step 5: The system verifies the new password and updates it for the selected account.* *Step 6: The system generates a confirmation message, indicating that the password has been successfully reset.* *Step 7: The password reset event is logged in the system's audit trail, recording details such as the administrator responsible, timestamp, and any relevant metadata for auditing purposes.* *Step 8: The administrator is returned to the main interface or account management section for further actions.*
Description of the Alternative Sequence	**Alternative Sequence 1**: If during the password reset process, the system encounters a critical error such as database connectivity issues or server malfunction, it halts the password reset process, displays an error message informing the administrator of the technical issue, and advises them to attempt the password reset again later or contact technical support for assistance.
Non functional requirements	- Reliability: The system should maintain consistent availability, minimizing downtime to ensure administrators can reliably reset passwords. - Usability: The password reset interface should be intuitive and user-friendly, guiding administrators through the process with clear instructions and minimal

	complexity. - Performance: The password reset process is expected to conclude within a specified duration of seconds. - Security: The security requirement for the password reset process ensures that only authorized administrators can reset passwords, preventing unauthorized access to user accounts.
Postconditions	1. The password for the selected account is successfully updated in the system's user database. 2. The system generates a confirmation message, notifying the administrator of the successful password reset. 3. The administrator is returned to the main interface or account management section for further actions.

The system shall grant administrators the capability to change the permission of accounts.

UC Name	*Admin Account Permissions Modification* *UC-206*
Summary	*Enabling administrators to modify permissions for user accounts.*
Dependency	*Admin Account Creation (UC-203)*
Actors	Primary Actor: User (Admin) Secondary Actor: System
Preconditions	*1. The administrator has appropriate access privileges and permissions to modify account permissions.* *2. The administrator is logged into the system.* *3. The system is operational and accessible.* *4. The administrator possesses all necessary information required to identify the account for which permissions need to be modified.*

Description of the Main Sequence	*Step 1: The administrator accesses the account management section of the system.* *Step 2: The administrator navigates to the list of user accounts and selects the account for which permissions need to be modified.* *Step 3: The system displays the current permissions for the selected account.* *Step 4: The administrator modifies the permissions as required.* *Step 5: The system verifies the modified permissions and updates them for the selected account.* *Step 6: The system generates a confirmation message, indicating that the permissions have been successfully modified.* *Step 7: The permission modification event is logged in the system's audit trail, recording details such as the administrator responsible, timestamp, and any relevant metadata for auditing purposes.* *Step 8: The administrator is returned to the main interface or account management section for further actions.*
Description of the Alternative Sequence	**Alternative Sequence 1**: If during the permission modification process, the system encounters a critical error such as database connectivity issues or server malfunction, it halts the process, displays an error message informing the administrator of the technical issue, and advises them to attempt the modification again later or contact technical support for assistance.
Non functional requirements	• Reliability: The system should maintain consistent availability, minimizing downtime to ensure administrators can reliably modify account permissions. • Usability: The permission modification interface should be intuitive and user-friendly, guiding administrators through the process with clear instructions and minimal complexity. • Performance: The permission modification process is expected to conclude within a specified duration of seconds. • Security: The security requirement for the permission modification process ensures that only authorized administrators can modify permissions, preventing unauthorized access to sensitive functionalities.

Postconditions	1. The permissions for the selected account are successfully updated in the system's user database. 2. The system generates a confirmation message, notifying the administrator of the successful permission modification. 3. The administrator is returned to the main interface or account management section for further actions.