System Requirements Statement (SRS) –

Roster Management Service

Created by : Swapnil Chandrakant Pawar

Pavan Ratnadip Pawar

Tanay Shrivastava

Rhutik Shirishkumar Salunkhe

Date : 20-July-2023

1. Introduction 3

2. Functional Requirements 4

2.1 Manager 5

2.2 Transport Authority 8

2.3 Employee 11

2.4 Use Case Diagram 1

# Introduction

The Roster Management Service Project is an innovative and essential initiative aimed at streamlining and optimizing the management of rosters within a dynamic and bustling environment. Rosters play a crucial role in transportation industry, this project seeks to develop a comprehensive and user-friendly system that automates and simplifies the process of assigning, monitoring, and coordinating rosters' tasks efficiently.

# Functional Requirements

|  |  |  |
| --- | --- | --- |
| **No** | **BRS requirement ID** | **Description** |
| **2.1** | **Module 1 Manager** | |
| **2.1.1** | **F1** | **User Registration** |
| **2.1.2** | **F2** | **User Login** |
| **2.1.3** | **F3** | **Role-Based Access** |
| **2.1.4** | **F4** | **Password Management** |
| **2.1.5** | **F5** | **Manage Accounts** |
| **2.1.6** | **F6** |  |
| **2.1.7** | **F7** |  |
| **2.2** | **Module 2 Transport Authority** | |
| **2.2.1** | **F11** | **User Registration** |
| **2.2.2** | **F12** | **User Login** |
| **2.2.3** | **F13** | **Task Prioritization** |
| **2.2.4** | **F14** | **Task Scheduling** |
| **2.2.5** | **F15** | **Task Assignment Automation** |
| **2.2.6** | **F16** | **Workload Balancing** |
| **2.2.7** | **F17** |  |
| **2.2.8** | **F18** |  |
| **2.2.9** | **F19** |  |
| **2.3 Module 3 Employee** | | |
| **2.3.1** | **F21** | **User Registration** |
| **2.3.2** | **F22** | **User Login** |
| **2.3.3** | **F23** | **Task Notifications** |
| **2.3.4** | **F24** | **Task Reports** |
| **2.3.5** | **F25** | **Task Status Updates** |
| **2.3.6** | **F26** | **Task Timeline** |

## Manager

* Employee Authentication and Access Control are essential components of the Roster Management Service, ensuring secure user access and appropriate permissions within the system. These functionalities empower Managers to manage user accounts efficiently.
* User Registration is a fundamental aspect of the system, allowing Managers to add new users to the platform. During the registration process, Managers can assign specific roles and permissions to each user, determining their level of access and functionality within the system. This enables a fine-grained control mechanism, ensuring that users have access only to the features and data relevant to their roles.

The Registration information consists of some items described as below.

1. First Name
2. Last name
3. E-mail ID
4. Password
5. User Type
   1. All items are compulsory demanded.
   2. First Name

* The First Name has constraints described as below.

1. Capital alphabet (A-Z)(first letter should be capital)
2. Small alphabet (a-z)(remaining letter should be small)
   1. Last Name

* The Last Name has constraints described as below.

1. Capital alphabet (A-Z)(first letter should be capital)
2. Small alphabet (a-z)(remaining letter should be small)
   1. E-mail ID

* If the Email ID correspond with not case-sensitive to other which is previously registered, the Email-ID should not be registered as an account.
  1. Password
* The Password has constraints which makes the Password consists of more than or

equal 8 and less than or equal 16 characteristics including characters described as below.

1. Numeric figure (at least one)
2. Capital alphabet (A-Z)(at least one)
3. Small alphabet (a-z)(at least one)
4. Special character (#, $, %, &, etc.) (at least one)

* The Password is masked by dummy characters. The re-entering Password is demanded.
  1. User Type

The User Type falls into two categories described as below.

1. Employee
2. Driver

* The User Type defines two types of users; "Employee", "Driver".
* Registration information should be entered on one screen and Login information should be entered on another screen after confirmed registration.
* The User Login functionality provides a secure gateway for registered users to access the system. Each user will have unique credentials, such as a username and password or the option for multi-factor authentication, to authenticate themselves securely. This authentication process safeguards against unauthorized access and maintains the confidentiality of sensitive data.
* The user authentication demands Email-ID and Password. The Email-ID and the Password should be checked in three ways.
  1. First, The Email-ID and the Password should be existed and correct.
* If The Email-ID and the Password are not equal to what the user has registered, the user authentication cannot be provided.
  1. Second, the User Type linked to the Email-ID should be "Tenant".
* When the User Type is "Employee", then user can be placed on “Employee’s Dashboard”.
  1. Finally, Email-ID should be available.
* The Manager can decide whether the Email-ID is available or suspended – Refer to the SRS of the Admin part.
  1. Password
* The Password has constraints which makes the Password consists of more than or equal 8 and less than or equal 16 characteristics including characters described as below.

1. Numeric figure (at least one)
2. Capital alphabet (A-Z)(at least one)
3. Small alphabet (a-z)(at least one)
4. Special character (#, $, %, &, etc.) (at least one)

* The Password is masked by dummy characters. The re-entering Password is demanded.
* Role-Based Access Control plays a pivotal role in governing user privileges. The system enforces role-based access, which means that each user's access rights are determined by their assigned role. For instance, Managers, Transport Authoritys, employees, and drivers may have different roles, each granting distinct levels of access to specific functionalities and data. This ensures that users can perform their designated tasks effectively while preventing unauthorized access to confidential information.
* Password Management is a critical component of user security. The system offers options for password reset, allowing users to regain access to their accounts in case of forgotten passwords. Moreover, stringent password complexity rules are enforced to enhance security, preventing the use of weak passwords that could compromise user accounts. These measures strengthen the system's overall security posture and protect against potential cyber threats.
* In conclusion, Employee Authentication and Access Control are pivotal elements of the Roster Management Service, prioritizing user security, seamless access, and appropriate privileges. By offering robust user registration, secure login, role-based access control, and enhanced password management, the system ensures that each user can perform their designated tasks efficiently while maintaining data confidentiality and integrity.

## Transport Authority

* User Registration is a fundamental aspect of the system, allowing Managers to add new users to the platform. During the registration process, Managers can assign specific roles and permissions to each user, determining their level of access and functionality within the system. This enables a fine-grained control mechanism, ensuring that users have access only to the features and data relevant to their roles.
* The Registration information consists of some items described as below.

1. First Name
2. Last name
3. E-mail ID
4. Password
5. User Type
   1. All items are compulsory demanded.
   2. First Name

* The First Name has constraints described as below.

1. Capital alphabet (A-Z)(first letter should be capital)
2. Small alphabet (a-z)(remaining letter should be small)
   1. Last Name

* The Last Name has constraints described as below.

1. Capital alphabet (A-Z)(first letter should be capital)
2. Small alphabet (a-z)(remaining letter should be small)
   1. E-mail ID

* If the Email ID correspond with not case-sensitive to other which is previously registered, the Email-ID should not be registered as an account.
  1. Password
* The Password has constraints which makes the Password consists of more than or

equal 8 and less than or equal 16 characteristics including characters described as below.

1. Numeric figure (at least one)
2. Capital alphabet (A-Z)(at least one)
3. Small alphabet (a-z)(at least one)
4. Special character (#, $, %, &, etc.) (at least one)

* The Password is masked by dummy characters. The re-entering Password is demanded.
  1. User Type

The User Type falls into two categories described as below.

1. Employee
2. Driver

* The User Type defines two types of users; "Employee", "Driver".
* Registration information should be entered on one screen and Login information should be entered on another screen after confirmed registration.
* The User Login functionality provides a secure gateway for registered users to access the system. Each user will have unique credentials, such as a username and password or the option for multi-factor authentication, to authenticate themselves securely. This authentication process safeguards against unauthorized access and maintains the confidentiality of sensitive data.
* The user authentication demands Email-ID and Password. The Email-ID and the Password should be checked in three ways.
  1. First, The Email-ID and the Password should be existed and correct.
* If The Email-ID and the Password are not equal to what the user has registered, the user authentication cannot be provided.
  1. Second, the User Type linked to the Email-ID should be "Tenant".
* When the User Type is "Employee", then user can be placed on “Employee’s Dashboard”.
  1. Finally, Email-ID should be available.
* The Manager can decide whether the Email-ID is available or suspended – Refer to the SRS of the Admin part.
  1. Password
* The Password has constraints which makes the Password consists of more than or equal 8 and less than or equal 16 characteristics including characters described as below.

1. Numeric figure (at least one)
2. Capital alphabet (A-Z)(at least one)
3. Small alphabet (a-z)(at least one)
4. Special character (#, $, %, &, etc.) (at least one)

* The Password is masked by dummy characters. The re-entering Password is demanded.
* Task Assignment Automation: The system shall automate task assignment using the task assignment algorithm, considering roster availability, proximity, and skill match.
* Workload Balancing: The system shall intelligently distribute tasks among available rosters to prevent overloading of individuals and ensure a balanced workload across the workforce.
* Task Prioritization: The system shall allow Managers and Transport Authoritys to assign priority levels to tasks, ensuring that high-priority tasks receive immediate attention.
* Task Scheduling: The system shall provide a user-friendly interface for task scheduling, allowing Transport Authoritys to allocate tasks and set deadlines efficiently.

## Employee

* User Registration is a fundamental aspect of the system, allowing Managers to add new users to the platform. During the registration process, Managers can assign specific roles and permissions to each user, determining their level of access and functionality within the system. This enables a fine-grained control mechanism, ensuring that users have access only to the features and data relevant to their roles.
* The Registration information consists of some items described as below.

1. First Name
2. Last name
3. E-mail ID
4. Password
5. User Type
   1. All items are compulsory demanded.
   2. First Name

* The First Name has constraints described as below.

1. Capital alphabet (A-Z)(first letter should be capital)
2. Small alphabet (a-z)(remaining letter should be small)
   1. Last Name

* The Last Name has constraints described as below.

1. Capital alphabet (A-Z)(first letter should be capital)
2. Small alphabet (a-z)(remaining letter should be small)
   1. E-mail ID

* If the Email ID correspond with not case-sensitive to other which is previously registered, the Email-ID should not be registered as an account.
  1. Password
* The Password has constraints which makes the Password consists of more than or

equal 8 and less than or equal 16 characteristics including characters described as below.

1. Numeric figure (at least one)
2. Capital alphabet (A-Z)(at least one)
3. Small alphabet (a-z)(at least one)
4. Special character (#, $, %, &, etc.) (at least one)

* The Password is masked by dummy characters. The re-entering Password is demanded.
  1. User Type

The User Type falls into two categories described as below.

1. Employee
2. Driver

* The User Type defines two types of users; "Employee", "Driver".
* Registration information should be entered on one screen and Login information should be entered on another screen after confirmed registration.
* The User Login functionality provides a secure gateway for registered users to access the system. Each user will have unique credentials, such as a username and password or the option for multi-factor authentication, to authenticate themselves securely. This authentication process safeguards against unauthorized access and maintains the confidentiality of sensitive data.
* The user authentication demands Email-ID and Password. The Email-ID and the Password should be checked in three ways.
  1. First, The Email-ID and the Password should be existed and correct.
* If The Email-ID and the Password are not equal to what the user has registered, the user authentication cannot be provided.
  1. Second, the User Type linked to the Email-ID should be "Tenant".
* When the User Type is "Employee", then user can be placed on “Employee’s Dashboard”.
  1. Finally, Email-ID should be available.
* The Manager can decide whether the Email-ID is available or suspended – Refer to the SRS of the Admin part.
  1. Password
* The Password has constraints which makes the Password consists of more than or equal 8 and less than or equal 16 characteristics including characters described as below.

1. Numeric figure (at least one)
2. Capital alphabet (A-Z)(at least one)
3. Small alphabet (a-z)(at least one)
4. Special character (#, $, %, &, etc.) (at least one)

* The Password is masked by dummy characters. The re-entering Password is demanded.
* Task Status Updates: The system shall allow rosters to update the status of assigned tasks (e.g., in progress, completed) in real time.
* Task Timeline: Managers and Transport Authoritys shall have access to a task timeline displaying key milestones, assignment times, and task completion times.
* Task Notifications: The system shall notify Transport Authoritys of any task delays or escalations, allowing them to take timely corrective actions.
* Task Reports: The system shall generate comprehensive task reports, including task completion rates, average task duration, and performance trends.

## Use Case Diagram

**Manager can access:**

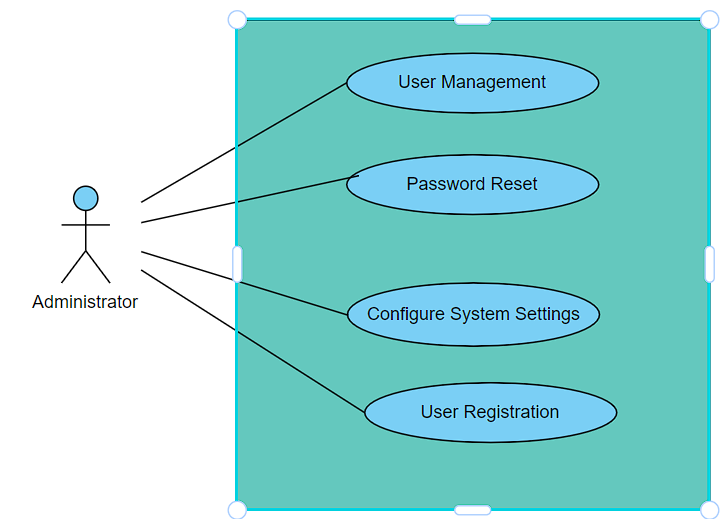
User Registration,

User Login,

User Management,

Configure System Settings,

Password Reset.



**Transport Authority can access**

User Registration,

User Login,

Task Assignment,

Task Monitoring,

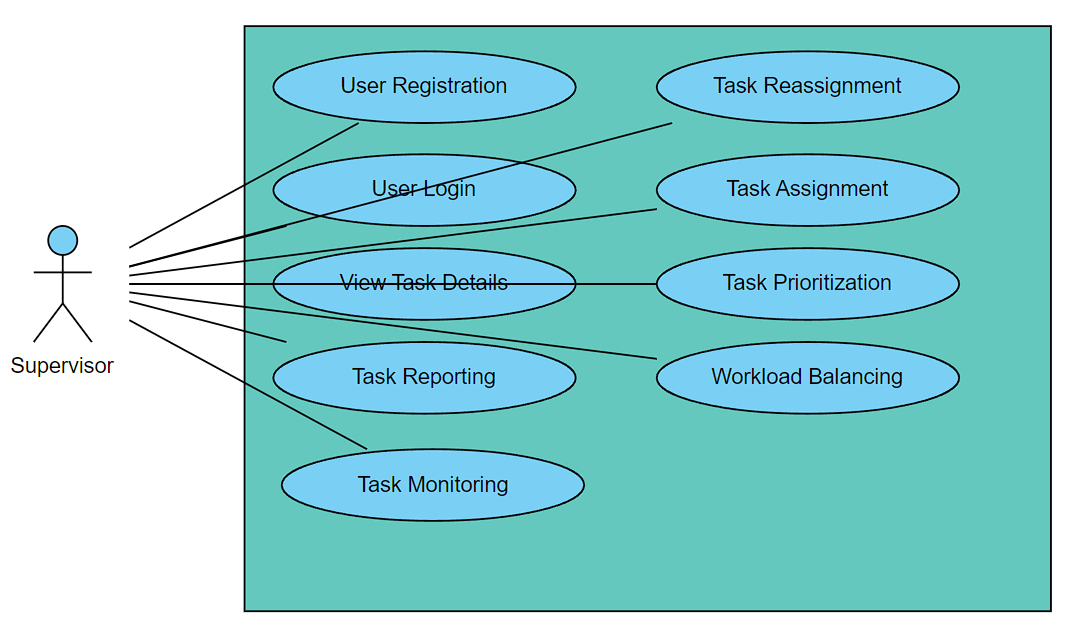
Task Prioritization,

Task Reassignment,

Task Reporting,

View Task Details,

Workload Balancing.



**Employee/Driver can access**

User Registration,

User Login,

Task Monitoring,

Task Reporting,

View Task Details.