Salez.ai -User Manual -V1.1

Document Control

Revision History

Date	Author	Version	Change Reference

Date	Author	Version	Change Reference
15 June -23	Muhammad Abdullah	1.0	Initial Draft
02- Aug -23	Ismail	1.1	Revised
20- Sep -23	Muhammad Abdullah	1.2	Revised

Introduction

The purpose of Salez.ai is to offer businesses a seamless and efficient one-stop solution, enabling customers to effortlessly access and leverage these software components from a single unified platform.

The scope of Salez.ai spans the entire sales and customer management spectrum, seeking to streamline processes and enhance operational efficiency for businesses. Salez.ai aims to empower organizations with actionable insights, providing them with a competitive edge in the market. With an emphasis on a centralized and user-friendly experience, Salez.ai facilitates improved sales operations, customer relationship management, and data-driven decision-making.

The scope of Salez.ai's offering extends to encompass the seamless integration of CRM, E-commerce, and POS functionalities, providing businesses with a holistic and efficient sales management solution. By offering a centralized platform for managing customer interactions, conducting online sales transactions, and facilitating in-store transactions, Salez.ai aims to simplify operations, reduce complexity, and ensure a smooth flow of data across different business functions.

Product Overview

Salez.ai is a comprehensive and integrated solution designed to provide businesses with a seamless and efficient one-stop platform for sales and customer management. The purpose of Salez.ai is to enable businesses to effortlessly access and leverage the combined power of Customer Relationship Management (CRM), E-commerce, and Point of Sale (POS) functionalities from a single unified platform.

Salez.ai is developed in three distinct phases, with each phase focusing on a specific Product. The first phase centres around the implementation of CRM functionalities. This includes managing customer interactions, tracking leads and opportunities, and enhancing customer engagement and retention strategies. By consolidating customer data and providing advanced CRM capabilities, Salez.ai enables businesses to effectively nurture customer relationships and drive sales growth.

The second phase of Salez.ai involves the development of E-commerce functionalities. This encompasses the creation of an online sales platform, including a product catalogue, shopping carts, secure payment processing, and order fulfilment capabilities. By integrating E-commerce functionalities into Salez.ai, businesses can seamlessly conduct online sales transactions, reach a broader customer base, and enhance their digital presence.

The final phase of Salez.ai focuses on the development of Point of Sale (POS) functionalities. This component enables businesses to process in-store transactions, manage inventory, generate sales reports, and facilitate a smooth checkout experience for customers. By incorporating POS functionalities, Salez.ai offers businesses a comprehensive sales management solution that covers both online and offline sales channels.

Deliverables

The following features are based on the initial scope defined and may need further collaboration to closely match the actual set of requirements

- UI Mockups/Design

- CRM (Customer Relationship Management)
- E-Commerce Platform
- POS (Point Of Sales) System

Functional Hierarchy

The CRM will have the following roles with different dashboards for each role

- System Administrator (Company Admin)
- Users (Created by Company Admin)

System Administrator (Company Admin)

The System Administrator, also referred to as the Company Admin, is a key role responsible for overseeing and managing the CRM system at an organizational level. This role possesses elevated privileges and holds the highest level of access within the system. The System Administrator's responsibilities include:

- Users Management
- Apps Management
- System Configuration
- Data Management
- Security and Permissions
- Customization

Users (Created By Company Admin)

Users are individuals within the organization who utilize the CRM system to perform their daily tasks and responsibilities. Users are created and managed by the System Administrator. Each user is assigned a specific role within the CRM system, which determines their access and limitations. Some key aspects of user roles include:

- Access and Permissions
- Limitations and Functionalities

Functional Hierarchy Diagram

After opening the application, the system administrator will be able to view the below-mentioned pages/screens:

Administrator Module

- Registration/Signup
  - Register themselves using the Signup Form
- Login
  - Login Via Username & Password
  - Email Verification
  - Remember Me Feature
- Forgot password
  - Username Validation
  - Email Reset Link Verification

Functional Details
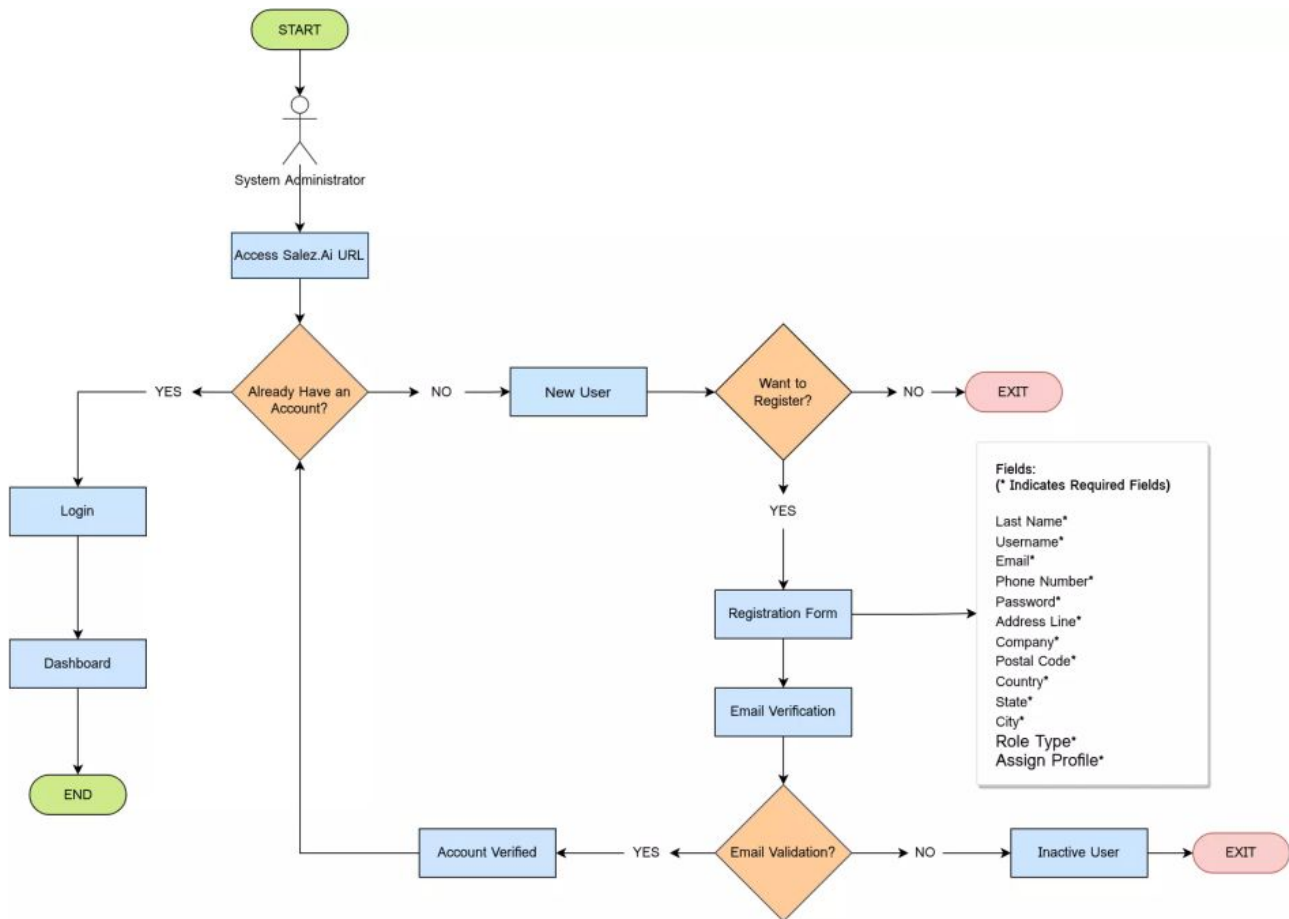
System Administrator (Company Admin)

Registration/Signup

To enhance user experience and provide system administrator with the convenience of self-registration, the platform offers a user-friendly interface that allows individuals to create their accounts easily. When the System Administrator creates a new account, the following fields will be available during the self-registration process:

(indicates required fields)*

- First Name*
  - The System Administrator needs to enter their first name.
  - Validation
    - The name should contain only alphabetic characters (letters) from the alphabet.
    - Special characters, numbers, and symbols are not allowed in the "First Name" field.
    - The field should not be left blank or contain any spaces.
- Last Name*
  - The System Administrator needs to enter their last name.
  - Validation
    - The name should contain only alphabetic characters (letters) from the alphabet.
    - Special characters, numbers, and symbols are not allowed in the "Last Name" field.
    - The field should not be left blank or contain any spaces.
- Username*
  - This field requires the system admin to enter their username.
  - Validation
    - Username must be in the format of email (i.e. **abc@company.com**).
    - This format ensures compatibility and adherence to the specific validation standards.
- Email*
  - It is mandatory for the system administrator to provide a valid and real email address during the account registration process.
  - The verification link is sent to the email address provided by the system admin during the registration process.
  - To complete the account verification process, the system administrator needs to click on the verification link received in their email. Account verification ensures the security of the registration process and helps prevent the use of invalid or reauthorized email addresses.
  - Validation
    - The account remains inactive until system admin will verify their account through the provided email address.
- Phone Number*
  - It is mandatory for the system administrator to provide a phone number during the account registration process.
  - Validation
    - There is a validation in place for phone numbers to ensure they do not exceed 15 digits. This validation serves to maintain data integrity and adhere to the standard format for phone numbers.
- Password*
  - This platform maintains strict security measures, and thus, system administrators are required to create a password that meets specific complexity requirements.
  - Validation
    - The password validation includes a minimum of 8 characters, at least 1 uppercase letter, 1 lowercase letter, 1 number, and 1 special character.
- Address*

- The System Administrator needs to enter their postal address, which is useful for contact and correspondence.
- Company*
  - The System Administrator needs to specify the name of the company or organization they are associated with.
- Postal Code*
  - The System Administrator needs to provide the postal code or ZIP code associated with their address.
- Country*
  - To enhance accuracy and ensure compatibility, the platform offers a user-friendly approach.
  - When the System Administrator enters the input field for the country. Instead of manually typing the country name, the system provides a convenient drop down menu that dynamically fetches a comprehensive list of countries using an API. So, The System admin can easily select their country of residence or operation from this list.
- State*
  - Upon selecting the country, the platform dynamically fetches a list of states or regions specific to the chosen country. The system Administrator can select the appropriate state from this list.
- City*
  - Similar to the state field, the city field presents a drop-down menu that dynamically populates the available cities based on the selected state. System Administrators can select their city from this list.
- Roles*
  - During self-registration, System Administrators are asked to choose their roles from a drop-down menu that contains the predefined list of basic profiles. Selecting a role helps us better understand their professional position within their organization.
    - CEO
    - CTO
    - Administrator
    - IT Manager
    - Business Development Manager
    - Sales Manager
- User Notification
  - After successful registration, Administrators will be presented with a popup message confirming the successful creation of their account. This popup serves as a notification that their account registration process has been completed successfully.
  - This popup includes essential details and instructions, such as a button labelled "Let's Get Started." By clicking on this button, the system administrator will be seamlessly redirected to the login page of the CRM system.
- Inactive User
  - In addition to the confirmation message, the platform sends a verification email to the provided email address. The verification email is an essential step in the registration process as it ensures the authenticity of the account and confirms the validity of the email address.
  - The accounts remains inactive until system admin will verify their account through the provided email address.
- User Flow Diagram
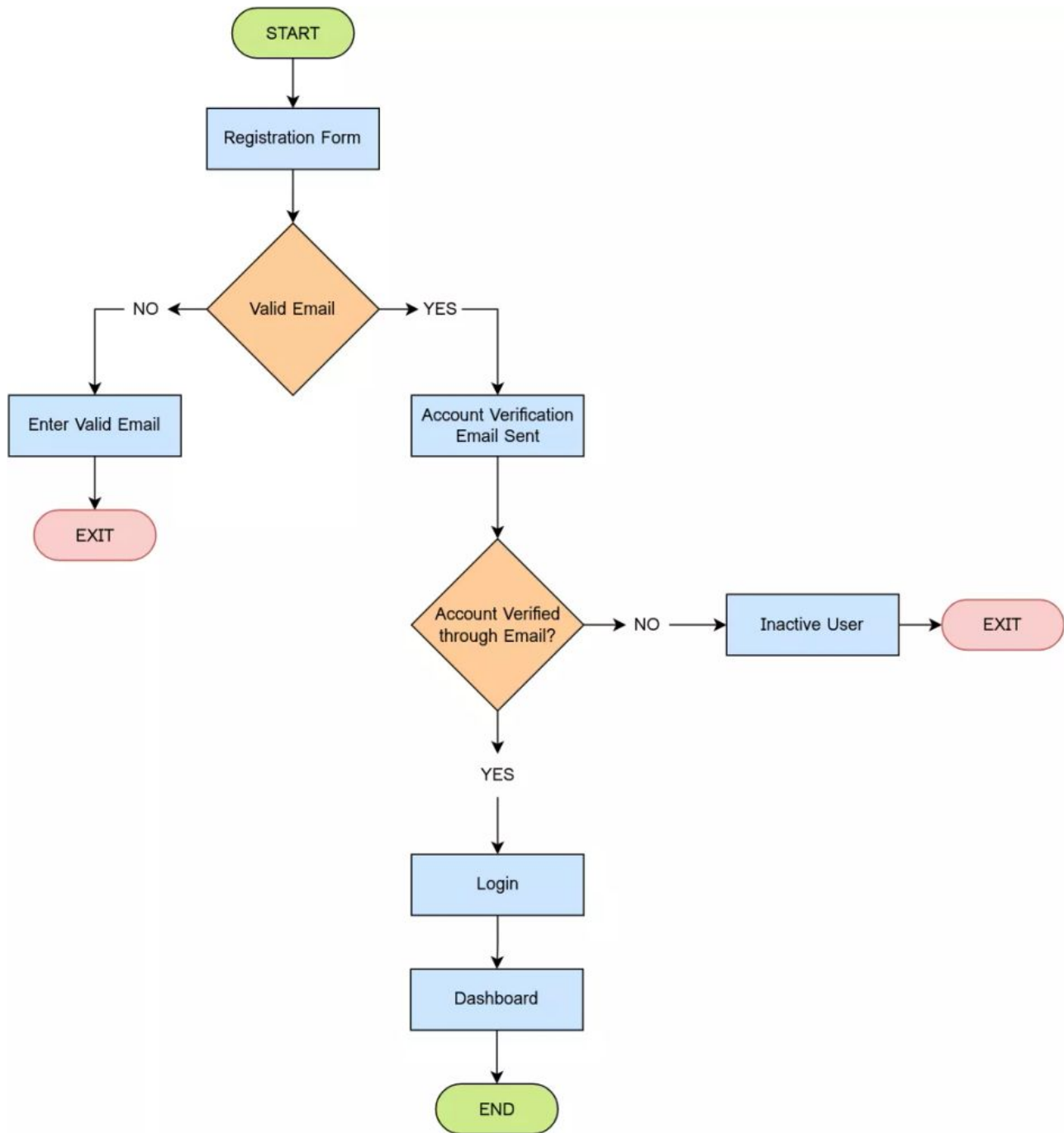
Registration/Signup Module - User Flow Diagram

Email Verification

Email verification is a crucial step in the signup process to ensure the validity and authenticity of the system administrator's accounts. After they provide their email addresses during the signup form, the CRM system implements an email verification mechanism to validate the provided email address. The process of email verification typically involves the following steps:

- Sending Verification Email
  - Upon completing the signup form, the CRM system generates and sends a verification email to the email address provided by the system administrator. This email contains a unique verification link.
- User Notification
  - The system displays a confirmation message to the system administrator, informing them that a verification email has been sent to their provided email address OR verify your user through email before logging in.
  - The system administrator has the time frame of 24 hours to verify that email address. After that, the email would be expired.
  - This message typically includes instructions to check their inbox, including the spam or junk folder if necessary, for the verification email.
- User Action
  - The system administrator is required to open the verification email and click on the provided verification link within a specified time-frame. This action confirms that the email address belongs to the system administrator and enables the system to mark the email address as verified.
- Verification Process
  - When the system administrator clicks the verification link, the CRM system verifies the authenticity of the email address. The system checks whether the provided information matches the records and confirms that the link is valid and has not expired.
- Account Activation

- Once the email address is successfully verified, the system administrator can be redirected to the page where the platform display the message that "Your Email is successfully verified" and the CRM system activates the system administrator account, granting them access to the system's features and functionalities.
- User flow Diagram
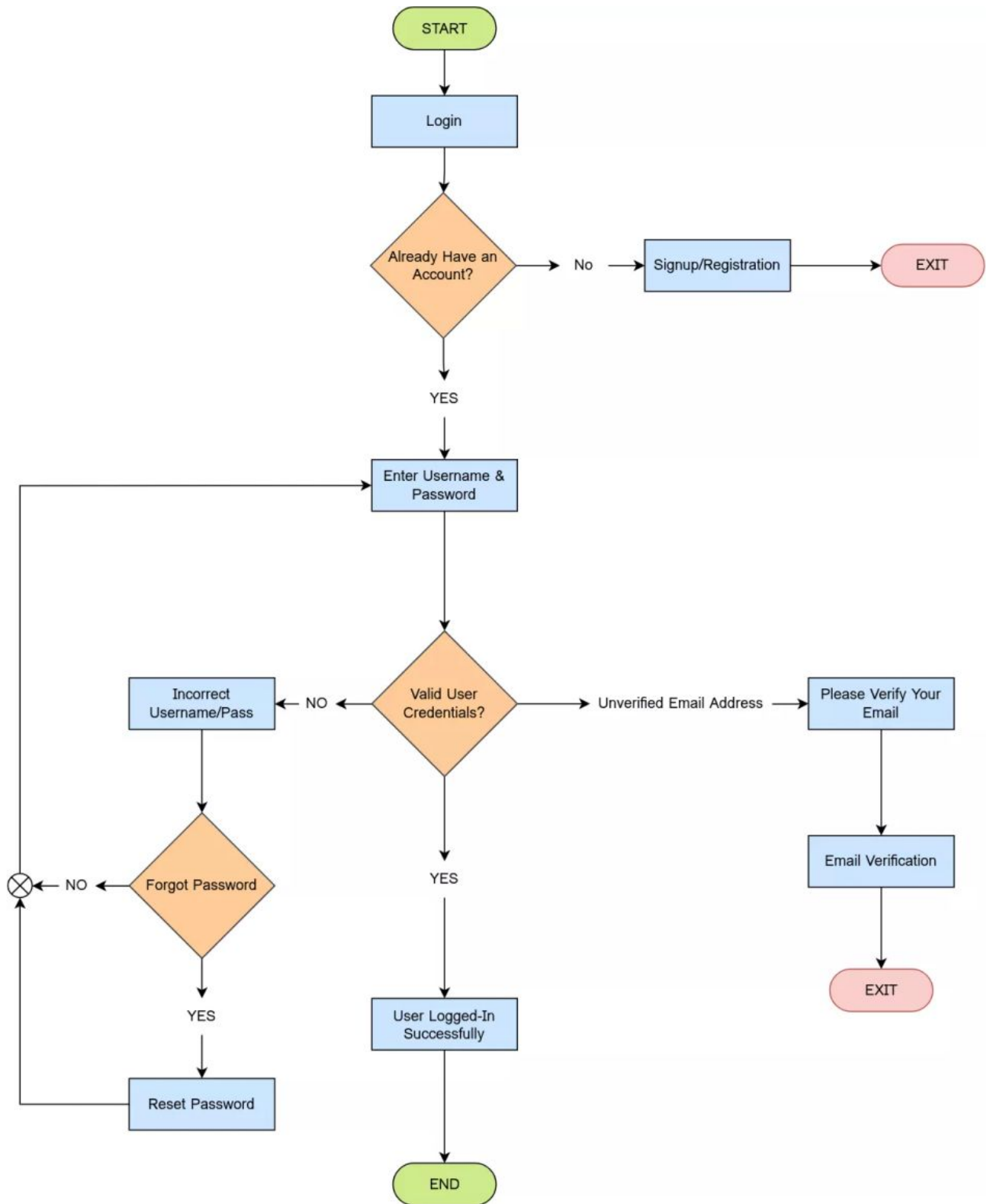

Email Verification Module - User Flow Diagram

Login

This module requires system administrators to provide their username and associated password in order to access their accounts. The login process follows these key steps:

- User Input
  - System Administrators needs to enter their username and associated password into the designated login fields on the platform's login page.

- Validation
  - The system verifies the entered username and password against the stored system administrator credentials.
- Successful Validation
  - If the provided username and password are successfully validated, system administrators are granted access to navigate to their Dashboard screen.
- Unverified Email Address
  - In the event that the email address is unverified, the system prompts system administrators to verify their email address.
  - The system administrator has the time frame of 24 hours to verify that email address. After that, the email would be expired. If system administrators have misplaced their verification link, they are given the option to request a new verification link to be sent to their registered email address. This ensures the security and accuracy of account information.
- Failed Validation
  - If the entered username and password do not match the stored credentials. The system displays an appropriate error message to the system administrator. The error message clearly communicates the reason for the login failure, providing guidance on the necessary steps to rectify the issue.
- Unmatched Email Address and Password
  - System Administrators are notified that the provided email address and password do not match. They are prompted to re-enter the correct credentials.
- Missing Email Address or/and Password
  - System Administrators are notified that the email address or password field is missing. They are prompted to provide the necessary information in order to proceed with the login process.
- "Remember Me" Feature
  - The "Remember Me" feature in the login screen is a functionality that allows users to opt for a convenient way to stay signed in to the CRM system without the need to manually enter their login credentials every time they access the application.
  - When users enable the "Remember Me" feature, the CRM system stores a persistent authentication token or cookie on their device. This token is used to automatically authenticate the user upon subsequent visits to the login screen, bypassing the need to enter their username and password.
- Doesn't Have an Account
  - If a system administrator lands directly on the login page and it doesn't have the account in the CRM then there is also an option of signup in the login screen.
  - When a user clicks on the "Signup" button, they are redirected to a registration form where they can enter details such as their name, email address, password, and any other required information.
- User Flow Diagram

Login Module - User Flow Diagram

Two-Factor Authentication

By Implementing two-factor authentication (2FA) module using a QR code to log into a Customer Relationship Management (CRM) system is a security measure that adds an extra layer of protection to user accounts. Here's how this process typically works:

- Assign Two Factor Authentication

- System Admin will be able to enable the Two-Factor Authentication against each pre-defined profiles within the CRM system by navigating to their security settings or preferences.
- Username and Password
  - The user initiates the login process by entering their username and password on the CRM login page.
- User Verification
  - The CRM system verifies the entered username and password against its database to ensure they are correct.
- QR Code Request
  - After successfully verifying the username and password, the CRM system shows the unique QR code that is generated against the session and it will regenerate after each 15 seconds in case of timeout.
- Scanning the QR Code
  - Using the 2FA authentication app, users scan the QR code displayed on the CRM login screen.
- Code Generation
  - Once the QR code is scanned, the 2FA app links to the user's CRM account and begins generating time-based one-time passwords (TOTPs).
- Access Granted
  - If the TOTP provided by the user matches the one generated by the app at that moment, they gain access to their CRM account.
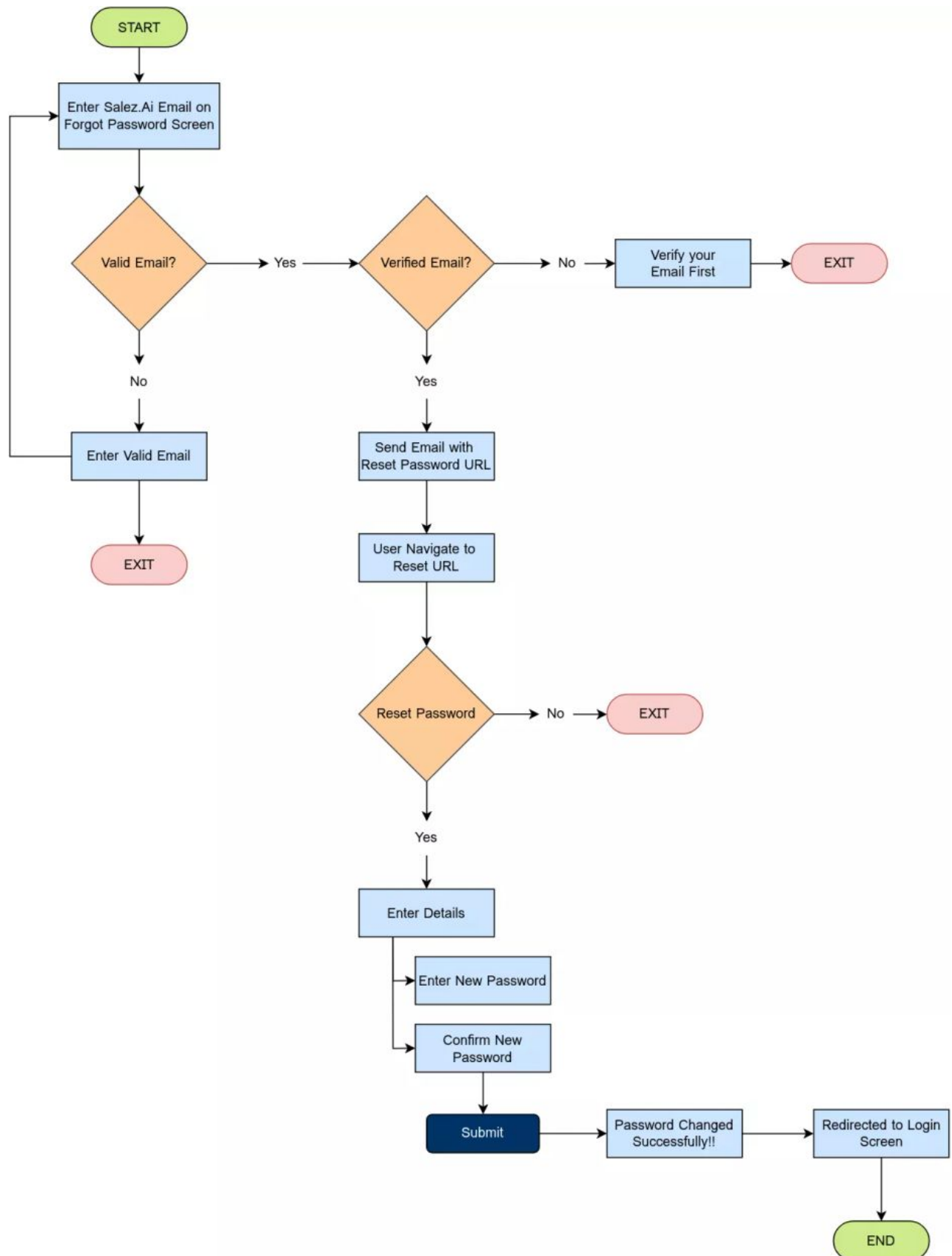
Forgot Password

This module allows system administrators to regain access to their accounts in the event of a forgotten password. The password recovery process follows these key steps:

- Password Recovery Request
  - Navigate to the login screen and clicks on Forgot Password button that leads to page on the platform and initiate a password recovery request by providing their registered email address.
- Email Verification
  - The system verifies the provided email address against the stored system administrator database to ensure its validity and association with an existing account.
- Password Reset Link
  - Upon successful email verification, the system generates a unique password reset link and sends it to the system administrator's registered email address. This link is time-limited up-to 15 minutes to ensure security and prevent unauthorized access.
- Incorrect Email Address
  - In case of an incorrect email address that does not match any existing email addresses stored in the system, an error message will be displayed in the form of a popup. The error message will indicate that the email address entered is incorrect or not found. This notification serves to alert the system administrator that the provided email does not correspond to any registered accounts in the system.
- User Notification
  - System Administrator receives an email containing the password reset link, along with instructions on how to proceed with resetting their password. The email also emphasizes the importance of keeping the password reset link confidential.
- Password Reset Page
  - Clicking on the password reset link button redirects to a secure password reset page on the platform. This page prompts the system administrator to enter a new password.
- New Password Creation
  - System Administrators are required to create a new password that meets the platform's password complexity requirements. The password should typically include a minimum number of characters, a combination of uppercase and lowercase letters, numbers, and special characters.
- Successful Password Reset

- Once system administrators submit their new password, the system securely updates their account with the newly chosen password. System Administrators are then notified of the successful password reset and prompted to log in using their updated credentials.
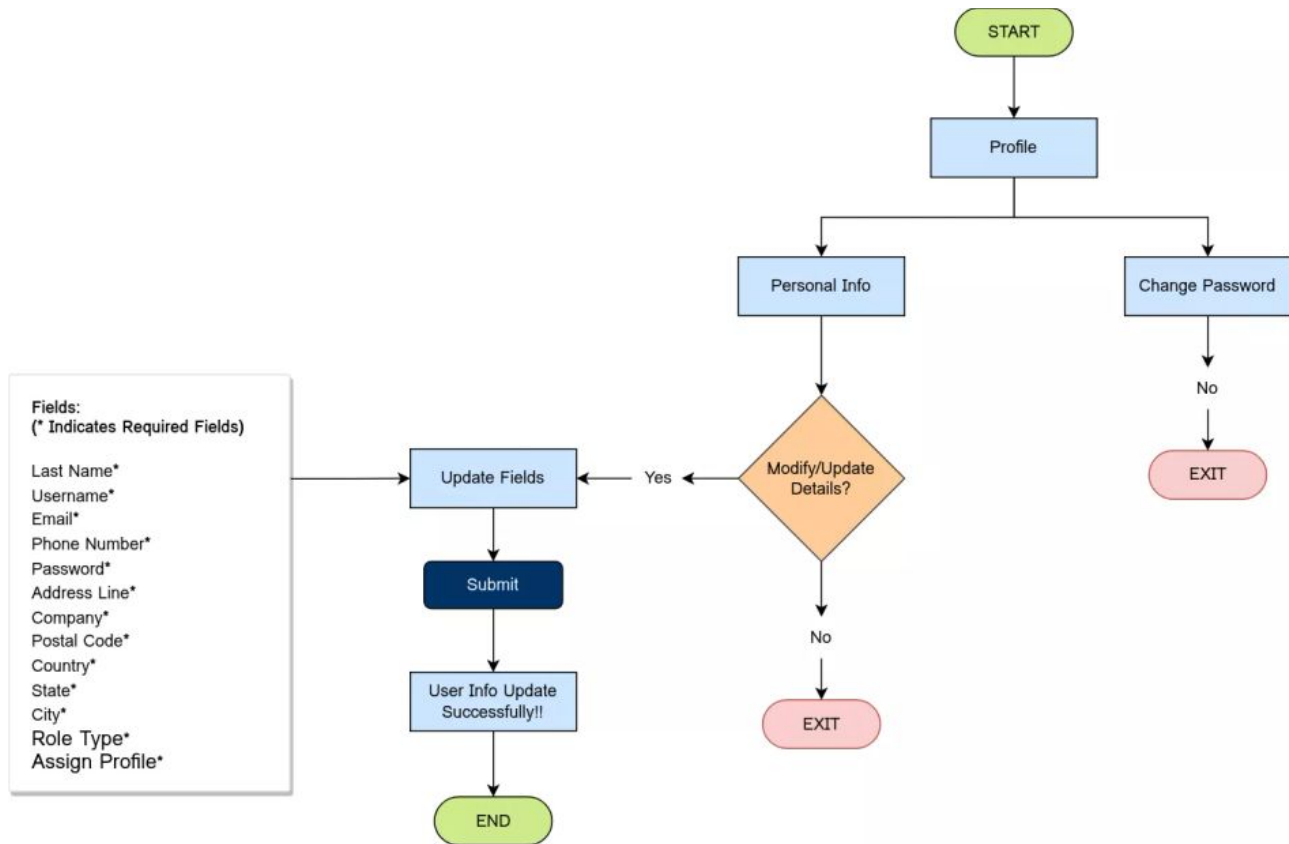- <u>User Flow Diagram</u>

Forgot Password Module - User Flow Diagram

Personal Information

When the System Administrator successfully logs in to their designated dashboard, they will find an option in the top right corner. Under the profile menu, they will be able to manage the following things,

- Manage Profile: View and Edit Personal Details:
  - The "Personal Details" section of the platform empowers administrators to view and modify their personal information for accurate record-keeping and profile management.
  - Within this section, administrators can access and update the following fields such as:
    - First Name
    - Last Name
    - Username (Changes the process of updating username)
    - Email
    - Phone Number
    - Password
    - Address
    - Company
    - Postal Code
    - Country
    - State
    - City
- Logout Feature:
  - The platform provides a Logout feature conveniently located under the profile menu. By selecting this option, the System Administrator can securely log out from their account, ensuring data privacy and enhancing the overall security of the CRM system. This feature offers a simple and effective way for the administrator to end their session and protect sensitive information when necessary.
- User Flow Diagram:

Edit/Update Personal Details - User Flow Diagram

Change Password

When a System Administrator wishes to modify their personal details, including changing the password of their account, the platform provides a user-friendly interface. To change the account password, the System Administrator should navigate to the "Change Password" tab, which is conveniently located next to the "Personal Details" section under the profile drop-down. Following this, they will need to proceed through the following steps:

- Current Password:
  - The System Administrator is required to input their current account password in this field to authenticate their identity.
- New Password:
  - In this field, the System Administrator can enter the new desired password for their account.
  - The new password must meet the platform's specified security requirements.
- Password Confirmation:
  - To ensure accuracy, the System Administrator is prompted to re-enter the new password in this field, confirming that they have typed the correct password.
- User Flow Diagram
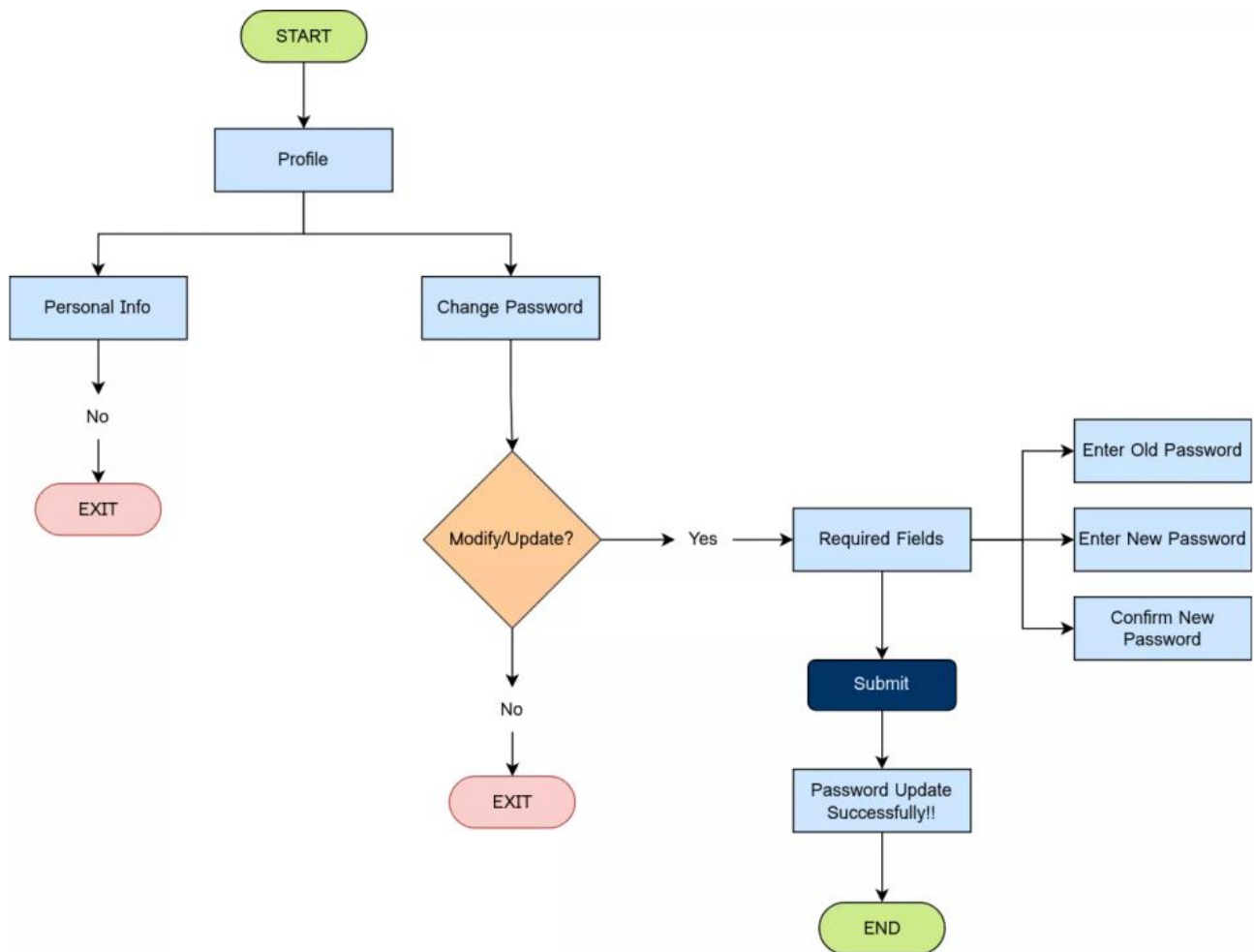
Change Password Module - User Flow Diagram

Login History

Under the "Change Password" fields. The system administrator will be able to see their login history that provides Administrators with a comprehensive view of their recent login activities. This section displays the following information:

- System Name:
  - The name or description of the system or device used for the login is shown, providing insight into the platform access points.
- Date and Time:
  - The exact date and time of each login activity are recorded, enabling customers to track their account access history.
- IP Address:
  - The IP address associated with each login event is displayed. This information helps customers identify any unauthorized access attempts or suspicious activity.

By providing a transparent Login History, our platform enables Administrators to monitor their account security and identify any potential unauthorized access.

Login Session Expired

A login session expiring typically means that the user's authenticated session has ended due to inactivity or a predefined time limit. When a user logs into the CRM, the system generates a session token or identifier that is associated with the user's authentication. This token is used to validate the user's access to the system and maintain their session.

When the login session expires, it means that the session token has expired, and the user is required to re authenticate to regain access to the CRM. This is a security measure to protect the user's account and data in case they leave their session unattended or if there are

concerns about unauthorized access.

- User Notification:
  - When a session expires there is a popup that displays the message/error of "Your Session Has Been Expired. Please Login Again!!" indicating that their session has expired. They will need to provide their login credentials again to establish a new session and continue using the CRM system.

User Management

User Management is a vital component of this CRM platform, designed to facilitate efficient administration and control of user accounts. These are the users that are created by the System Administrators. It encompasses various features and functionalities that empower administrators to manage user roles, profiles, user lists, and groups effectively. Administrators can create and manage these that are mentioned below:

- Roles Management
- Profiles Management
- Users Management
- Groups Management
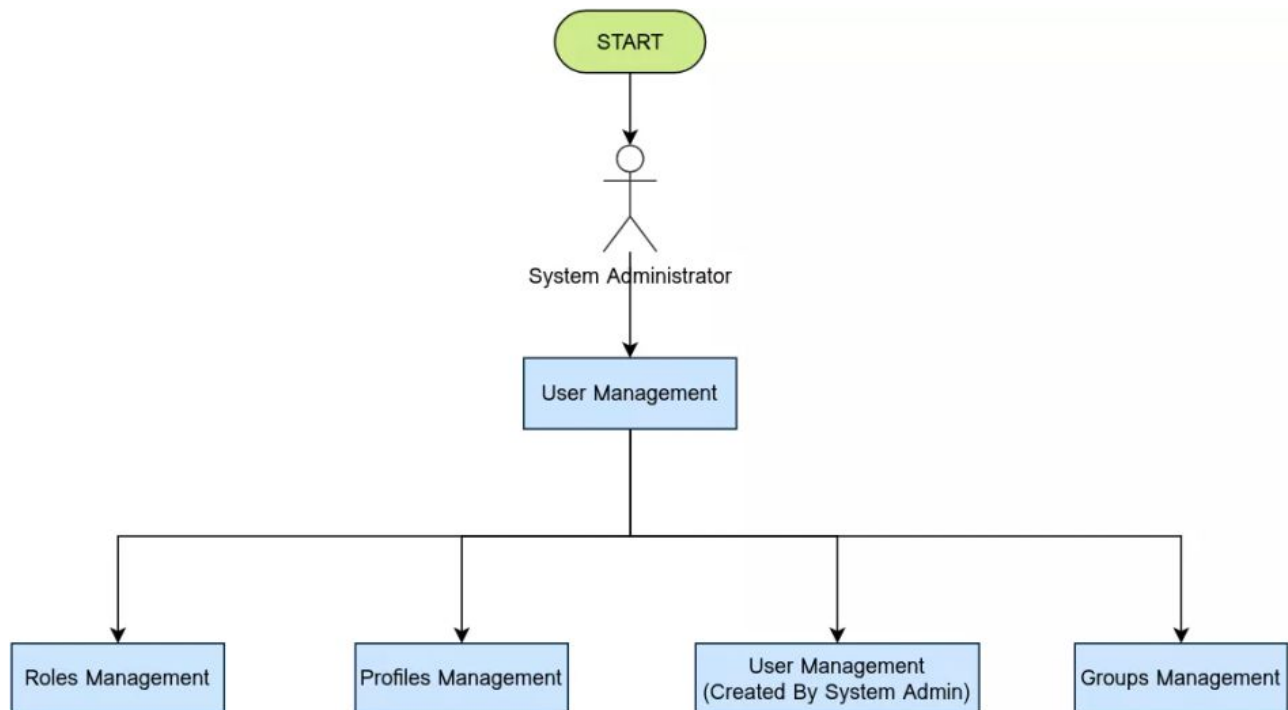
Roles Management:

The CRM system incorporates a comprehensive Roles Management feature that enables users to effectively manage and administer roles within the organization. This feature provides the necessary tools and functionalities to create, assign, modify, and maintain roles, ensuring proper access control and streamlined operations. There is a toggle button by which the system administrator can see and manage the "View Tree Structure" OR "View Role Hierarchy". The Roles Management module consists of the following key aspects:

- **View Tree Structure:**
  - The CRM system incorporates a view tree structure that represents the basic hierarchy of the organization and allows Administrators to expand or collapse the roles for clear visualization of the organizational structure and reporting relationships**.**
    - **Basic Hierarchy of Organization:**
      - The view tree structure in the CRM system presents a visual representation of the organization's hierarchy. It showcases the relationships and reporting lines between different roles and individuals within the organization. The hierarchy typically starts

with the highest-level roles, such as the CEO or top-level executives, and extends down to lower-level roles and employees.

- **Expand/Collapse the roles:**

  - Within the view tree structure, Administrators can expand or collapse the roles displayed. This feature allows administrators to selectively view or hide specific roles within the hierarchy, depending on their needs or the level of detail required. By expanding a role, administrators can view the individuals associated with that role, their reporting relationships, and any subordinate roles.

- **View Role Hierarchy:**

  - Within the CRM system, Administrators can view and manage the role hierarchy, which represents the organizational structure and reporting relationships. By accessing the "View Role Hierarchy" feature, they can navigate through the hierarchy through the toggle button and perform various actions related to roles and record types.

    - **Add Parent Role:**

      - To modify the role hierarchy, they can choose to add a parent role by clicking on the "Add Parent Role" option. This action prompts a popup where they can enter the role label and name for the new parent role. These are the details required when the administrator tried to add the parent role. Once the details are entered, Popups come for the success of the addition of a parent role.

    - **Add Record Type:**

      - Another functionality available within the role hierarchy is the management of record types. Administrators can add a new record type by selecting the "Add Record Type" option. In the corresponding popup, users can enter the following information:
        - Enter Role Label
        - Enter Role Name
        - Save/Cancel Popup

    - **Delete Record Type:**

      - In addition to adding record types, Administrators have the option to delete existing record types. When selecting the "Delete Record Type" option, a validation prompt appears, asking users to confirm the deletion. Users can choose either "Yes" to proceed with the deletion or "No" to cancel the operation.
        - Record Delete Validation (Yes/No)

    - **Modify/Update Record Type:**

      - Furthermore, Administrators can update or edit existing record types by selecting the "Update/Edit Record Type" option. This action opens a popup where Administrators can modify the role label and name of the record type. In the corresponding popup, they can enter the following information:
        - Update Role Label
        - Update Role Name

    - User flow Diagram:
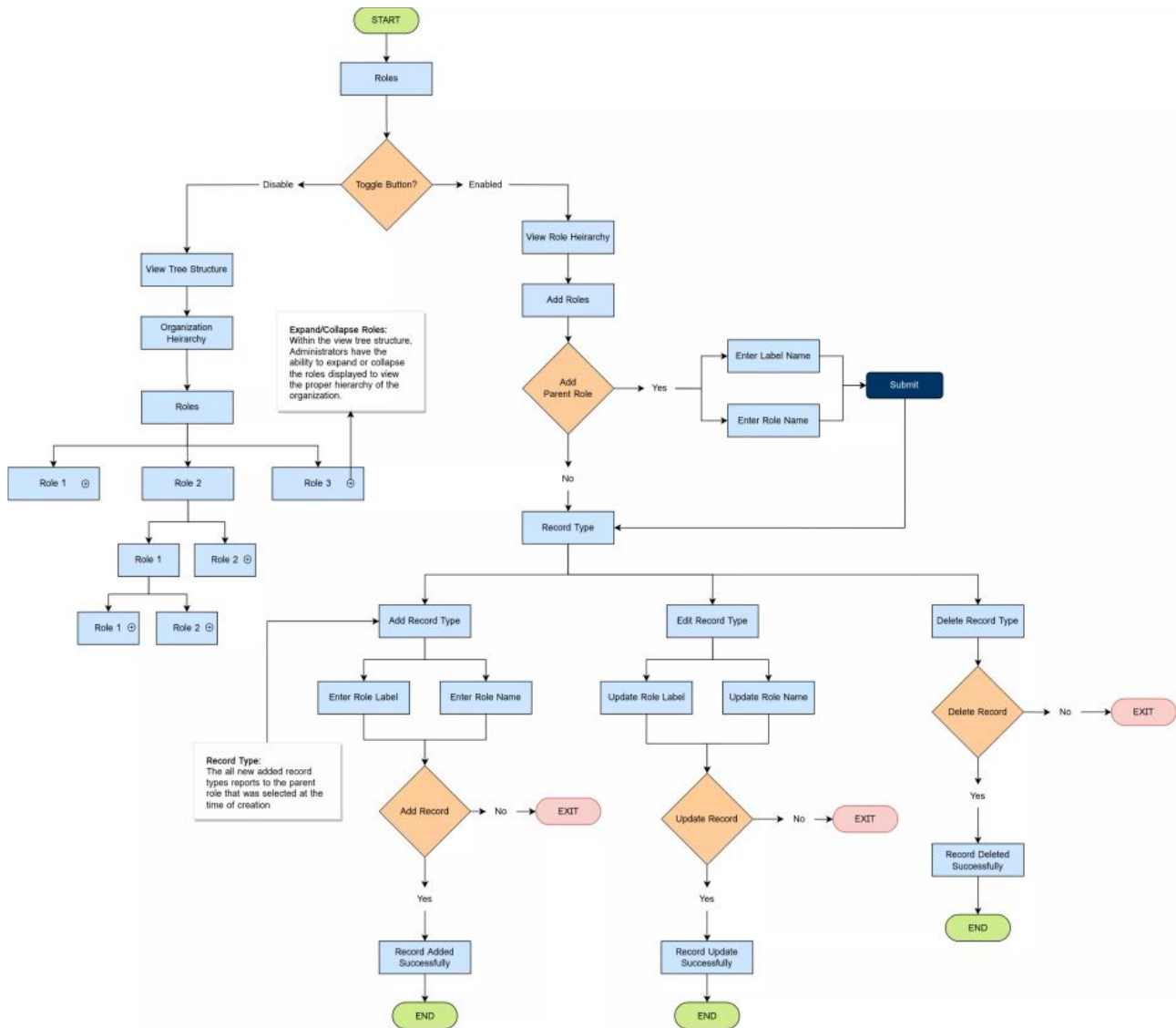
Roles Management - User Flow Diagram

Profile Management

In the CRM system, the Profiles Management feature empowers system administrators to finely control access permissions related to apps, system configurations, and side menu settings. System administrators create profiles as templates, each pre-configured with specific permissions. These permissions dictate the extent of access and functionality granted to all users linked to these profiles. The Profiles Management module includes the following key functionalities:

Profile Creation

When adding a profile, the following steps and options are available:

- **Enter Profile Name:**
  - To create a new profile in the CRM system, the System Administrator initiates the process by clicking on the 'Add Profile' button.
  - This action triggers the appearance of a modal window, prompting the System Administrator to enter the desired profile name and then proceed with saving it.
    - **Validation:**
      - Profile name must be unique and profile does not create if the profile already exists with the same name. This serves as a label to identify and distinguish the profile from others within the CRM system.
      - If an system administrator attempts to create a profile with a name that already exists in the system, a validation error occurs, and a prompt displays an error message stating "Profile Name should be Unique."

- The profile name field must be completed and cannot be left empty. When a user attempts to proceed without filling in such a field, the system will prompt the user to provide the necessary information. For instance, if the field is left blank, the system will display a prompt urging the user to enter their name before proceeding.
  - **Successful Profile Creation:**
    - Upon successfully creating a profile, system administrator receive a confirmation message in the form of a popup, indicating that the profile has been successfully added to the system. This notification ensures that system administrator is aware of the successful profile creation and can proceed with further actions.
    - After the profile creation, the system automatically redirects the administrator to the detail page of the newly created profile. From this detail page, he can manage following things,

- **App Settings - Permissions:**

In this section, the System Administrator can assign specific apps to a profile. Once an app is assigned to a profile, all users associated with that profile gain access to various features, including app editing, module management, view customization, view type selection, section and field management, among others. In this section, the System Administrator can efficiently manage the following aspects:

- **Assigned Multiple Apps:**
  - The Administrator navigates to the app assignment section. Within this section, he will find a list of available apps along with check-boxes next to each app name. By selecting the check-boxes for the desired apps, the Administrator can assign those apps to the profile and that apps would be accessible to all the users that are lies under that profile.
    - **By Default (Only One):** By this Feature, Administrators can specify that only one default app is assigned to the profile, ensuring a focused user experience.
    - **Visible (Multiple):** Administrators can choose to make multiple apps visible to the profile, allowing users assigned to the profile to access and utilize those apps.

- **System Settings - Permissions:**
  - In this section, administrators can configure various permissions related to system settings for the profile. These settings reflects the same to all the users that are associated with that profile. The following options are available within this section:
    - **Allow two-Factor:**
      - System Administrator can enable or disable the two-factor authentication for profiles by clicking the checkbox present next to "Allow Two Factor" to enhanced security.
      - Enabling the checkbox triggers the display of a QR code.
      - Users will see this QR code on their screen after entering their username and password during their next login, once two-factor authentication is enabled.
      - The QR code is regenerated automatically after a specific duration of time. This periodic regeneration enhances security by providing users with fresh QR codes at regular intervals.
      - Users need to install a 2FA authentication app (e.g., Google Authenticator, Authy, Microsoft Authenticator) on their trusted mobile device to scan the QR code.
    - **Password expire in (Days):**
      - This field display the drop-down menu with these options from which the System Administrator can set the minimum and maximum number of days for password expiration for a specific profile. This policy implements on all the users associated with the selected profiles on which the system administrator enables this feature:
        - 30 days
        - 60 days
        - 90 days
        - 180 days
        - One year
        - Never Expires
      - **Password Expiration Policy:** System Administrator can configure password expiration policies for different profiles. For instance, they can set a policy that requires users to change their passwords every 90 days.

- **User Login:** Let's say a user logs in for the first time with their initial password. The CRM system recognizes that this password has an expiration policy and calculates the date when it will expire based on the policy settings.
- **Notification Period:** Salez.Ai typically provides users with a notification period before their password expires. This is often set a few days before the actual expiration date, for example, five days. During this notification period, if a user logs in (let's say on the 85th day since their last password change), they will receive a notification.
- **Password Change Process:** When the user follows the link or prompt, they are taken to a password change page. Here, they must enter their current password (the one that's about to expire) and then create a new, secure password that meets the organization's password policy requirements (e.g., a combination of letters, numbers, and special characters).
- **Successful Change:** Once the user successfully changes their password, they can continue to access Salez.Ai as usual with the new password. The password expiration date is reset based on the policy settings, starting from the date of the password change.
- **Expired Password:** If the user does not change their password during the notification period and the password expires, they will not be able to log in. They'll be locked out of their account until they follow a password reset process, they will see the modal at the time of the login to their account to setup your new password with the following fields,
    - Enter New Password
    - Confirm New Password
- **New Expiration Date:** If password expiration policy is set for 90 days, and the user change his password on the 30th day, then new password's expiration date should be calculated from the date the user changed it. New password's expiration date would be 90 days from the date when user changed his password.
  - **Invalid login attempt:**
    - Administrators can define the minimum and maximum number of invalid login attempts allowed for each profile. These login attempts validation implements on all the users associated with that profile. After exceeding this limit, they may be locked out of their accounts temporarily and they needs to contact the administrator to regain the access again.
    - This field display the drop-down menu that contains the following number of attempts that are allowed to try. The invalid login attempts that are display in the drop-down menu are,
      - 3
      - 5
      - 10
      - No Limits
  - **Minimum password length:**
    - Administrators can specify the minimum and maximum required length for passwords associated with the profile, ensuring adherence to password security best practices. The same validation implements on all the users associated with that profile.
    - The minimum and maximum required length for passwords are,
      - 8 characters
      - 12 characters
      - 16 characters
  - **Report create:**
    - Administrators can grant or restrict the ability to create reports assigned to the profile by enabling or disabling this option.
  - **Report run:**
    - Administrators can determine whether profiles can run reports or not by enabling or disabling this option.
  - **Edit Mode Access:**
    - Administrators possess the capability to control access to the Edit Mode Screen for specific profiles by toggling a checkbox.
    - Enabling the checkbox grants the profile access to the Edit Mode Screen of the corresponding app, whereas disabling the checkbox restricts this access. When the checkbox is disabled, the toggle button for entering the Edit Mode Screen becomes unavailable for that particular profile.
- **Side Menu Settings (Assigned items in the side menu):**

- In profile management, administrator can access the Side Menu Settings section, where they will find a list of menu items corresponding to various functionalities and features.
- The Administrator can easily restrict the users that are associated with the profiles to a certain level of permissions and visibility by using the check box that is shown against each menu item in the Side Menu Settings
- When a checkbox is selected, it indicates that the corresponding menu item is visible and accessible to the user associated with that profile. Conversely, when a checkbox is deselected, it restricts the visibility and access of that menu item for all that users that belongs to that profile.
- The menu items that can be managed in the Side Menu Settings section using the Checkbox includes:
  - Apps
  - Dashboard
  - User Management
    - User List
    - Profiles
    - Roles
    - Groups
- Setting
  - App settings
  - Web to lead
  - Lead Mapping

List All Profiles

The CRM system provides a comprehensive feature to list all profiles within the platform. When accessing the "List All Profiles" section, system administrator is presented with a table or list displaying the profiles. The following information is typically included for each profile:

- **Date of Creation:**
  - This column displays the date on which the profile was created by the system administrator. It provides them with a reference point for understanding the timeline of profile creation.
- **Name:**
  - The name column showcases the unique identifier or label assigned to each profile. It helps system administrator quickly identify and differentiate between different profiles.
- **Action (Update & Modify Profile):**
  - Under the action column, system administrator can perform various actions specific to each profile. These actions typically include options to update or modify settings associated with the profile. For each profile, The system administrator has the option to updates the following settings and permissions:
    - App Settings
      - Updated Assigned Apps
    - System Settings
      - Allow two-Factor
      - Password expire in (Days)
      - Invalid login attempt
      - Minimum password length
      - Report create
      - Report run
      - Edit Mode Access
    - Side Menu Settings
      - The menu items that can be managed in the Side Menu Settings section using checkboxes include:
   - Apps

- Dashboard
- User Management
  - User List
  - Profiles
  - Roles
  - Groups
- Setting
  - App settings
  - Web to lead
  - Lead Mapping

Filters

- **Search Filters**
  - The CRM system incorporates a powerful filtering feature that allows administrators to refine their search and retrieve specific profiles based on various criteria. The Filters functionality within the CRM system includes the following options:
    - Filter By Name
      - The System Administrator can apply a name filter to search for profiles by entering specific keywords or names associated with the profiles. This filter typically provides an input field where they can enter the desired name or keyword to narrow down the search results.
    - Filter By Date
      - The CRM system offers a date filter that allows administrators to filter profiles based on the date of creation. This filter is typically facilitated through a calendar interface where they can select a specific date or a range of dates to filter the profiles accordingly.
    - Reset Filter
      - To clear all applied filters and start a new search, Administrators can utilize the "Reset Filter" option. This function removes any previously set filters and resets the profile list to its original state, enabling them to perform a fresh search without any applied filters.

Userflow Diagram:
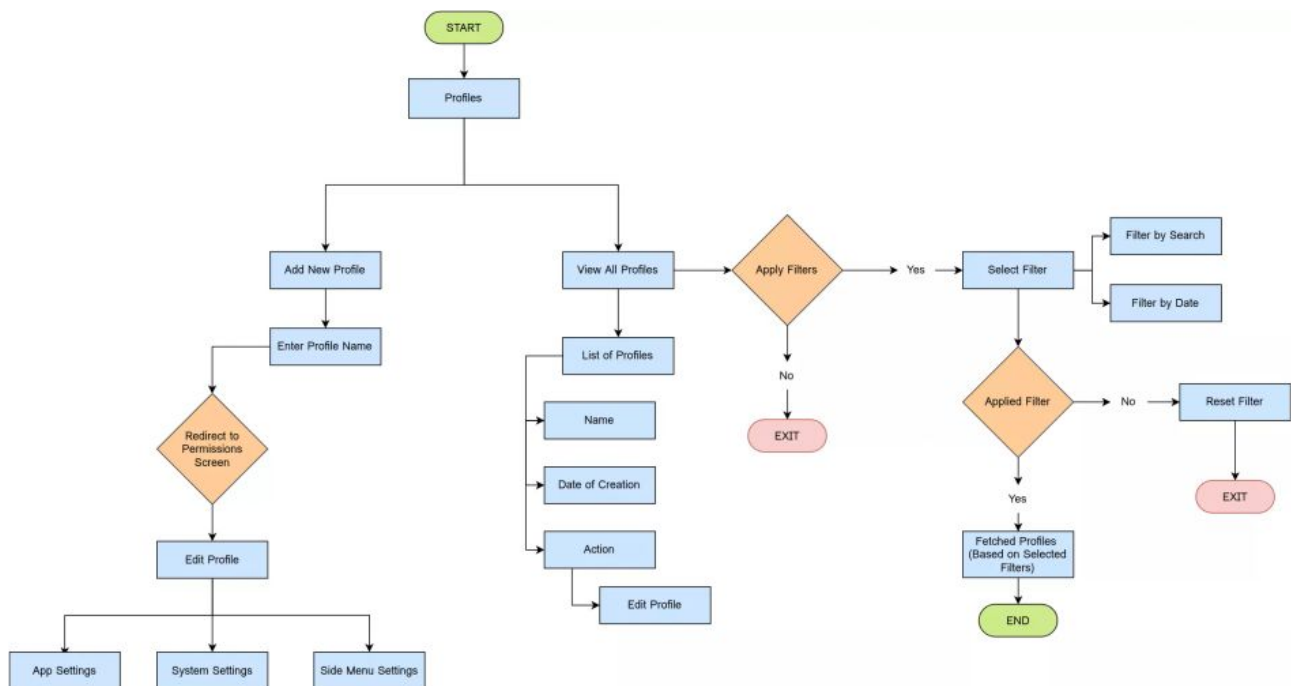
User List Management

User List Management in the CRM system refers to the functionality that allows administrators or authorized users to view, organize, and manage the list of users within the platform. It provides a centralized view of all users and their associated details, facilitating efficient user administration and access control. The User List Management typically includes the following features:

- **Search Filters**
  - User List Management in the CRM system includes various filters and options to effectively manage and search for users. The following features are available:
    - **Filter By Name:**
      - Administrators can apply a name filter to search for specific users by entering specific keywords or names associated with the users. This filter typically provides an input field where users can enter the desired name or keyword to narrow down the search results.
    - **Filter By Date:**
      - The CRM system offers a date filter that allows users to filter users based on the date of creation. This filter is typically facilitated through a calendar interface where Admins can select a specific date or a range of dates to filter the profiles accordingly.
    - **By All:**
      - This option allows admin to view all user profiles without any specific filtering criteria. Within the "By All" filter option, users have additional sub-options to further refine their search:
        - **All:**
          - This option displays all user profiles, regardless of their verification status.
        - **Verified:**
          - This option shows only the user profiles that have been verified.
        - **True:**
          - This option filters the user profiles to display only those with a "true" status based on a specific attribute or condition.
        - **False:**
          - This option filters the user profiles to display only those with a "false" status based on a specific attribute or condition.
    - **Reset Filter:**
      - To clear all applied filters and start a new search, users can utilize the "Reset Filter" option. This function removes any previously set filters and resets the profile list to its original state, enabling users to perform a fresh search without any applied filters.
- **List All Users (Created By Admin)**
  - The CRM system provides a comprehensive list of all users created by the administrator. This user list displays important details for each user profile, including
    - **Name:**
      - The name of the user, which could include the first name and last name.
    - **Username:**
      - The unique username associated with the user's account. This is used for authentication and login purposes.
    - **Email:**
      - The email address registered for the user's account. This serves as a primary contact method for communication.
    - **Phone Number:**
      - The phone number provided by the user during registration. This contact information allows for direct communication if required.
   - **Date of Creation:**
      - The specific date when the user profile was created in the CRM system. This information helps in tracking the timeline of user registrations.
    - **Verified:**

- It indicates whether a user's email address has been verified or not. This field serves as a status indicator to determine if the user has completed the email verification process.
  - **Freeze:**
    - There is a "Freeze" field that allows administrators to see the statuses of the user accounts whether they are frozen or not. If the user can exceed the number of the Invalid login attempts then their accounts would be temporarily frozen. The "Freeze" field serves as a control mechanism to temporarily restrict the functionality or access of a user account.
  - **Actions:**
    - **View:**
      - The "View" action allows administrators to access and view the details of a specific user account. By selecting the "View" option, administrators can retrieve information such as the user's name, email address, phone number, role, and other relevant details.
    - **Edit:**
      - The "Edit" action enables administrators to modify and update the information associated with a user account. By selecting the "Edit" option, administrators gain access to an editable form or interface where they can make changes to fields such as the user's name, email address, phone number, role, and other relevant details.

- **Add New User**
  - To streamline the process of adding new users to the CRM system, an intuitive interface is provided. When adding a new user, the following fields are required to be completed:
    - First Name
    - Last Name
    - Username
    - Email
    - Phone Number
    - Password
    - Address Line
    - Company
    - Postal Code
    - Country
    - State
    - City
    - **Role Type:**
      - The assigned role for the user, chosen from a list of available roles fetched from the system.
    - **Assign Profile:**
      - The selected profile to assign to the user, chosen from a list of available profiles fetched from the system.

Userflow Diagram:
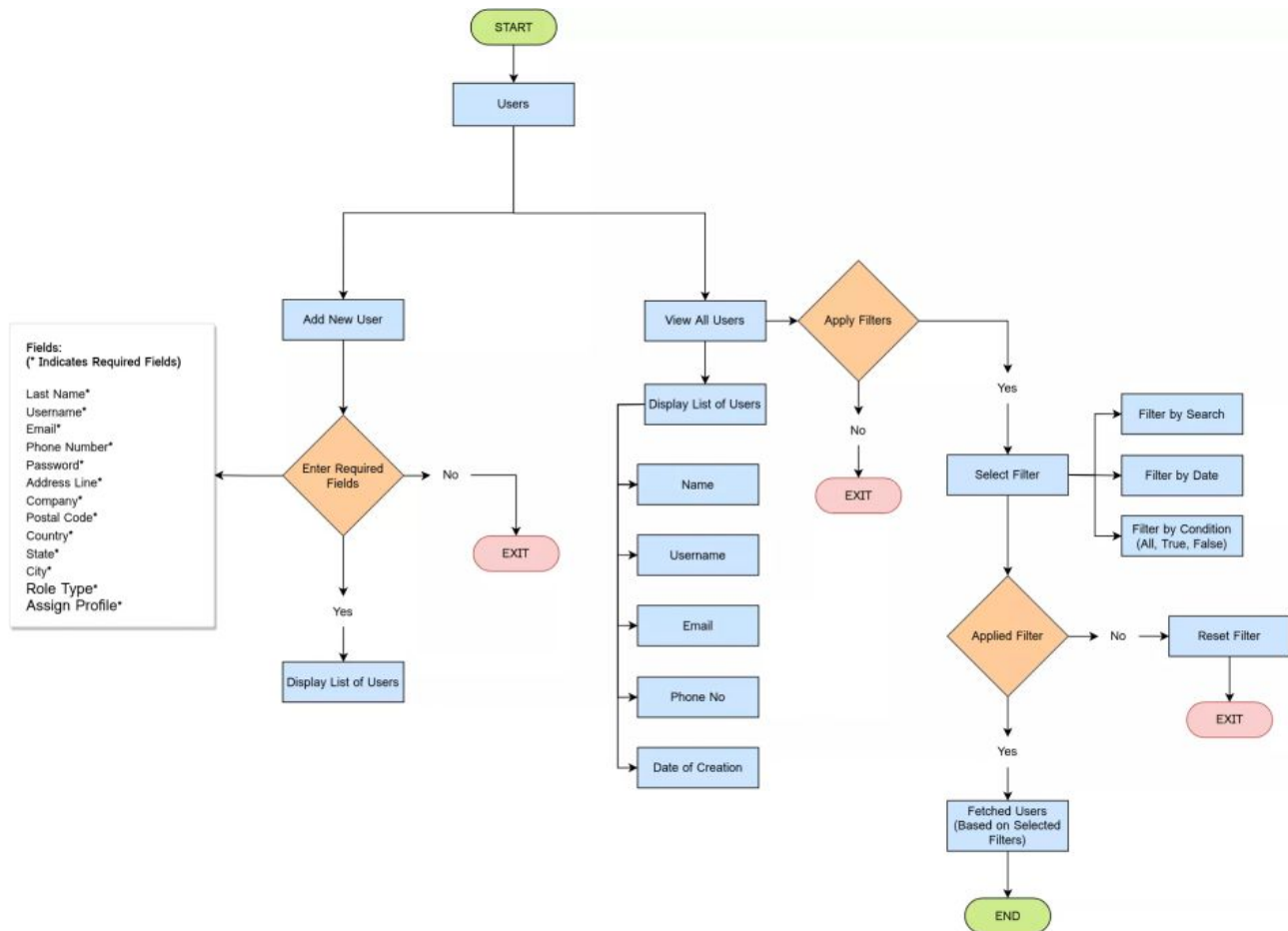
User List Management - User Flow Diagram

Group Management

The CRM system refers to the capability of creating, organizing, and managing groups within the platform. A group is a collection of users or entities with shared characteristics, allowing for easier management and collaboration. Group Management provides administrators and users with the ability to create, modify, and delete groups, as well as assign members to these groups.

- **Search Filters**
  - In the CRM system, the Groups Management feature allows users to organize and manage groups effectively. To enhance the usability of this feature, the system provides various filters to facilitate easy searching and filtering of groups. The available filters include
    - Filter By Name:
      - This filter allows users to enter specific keywords or names associated with groups in an input field. It helps narrow down the search results and retrieve groups with matching names.
    - Filter By Date:
      - The CRM system enables users to filter groups based on the date of creation. By using a calendar interface, users can select a specific date or a range of dates to filter the groups accordingly. This is particularly useful when searching for groups created within a specific time frame.
    - Reset Filter:
      - The "Reset Filter" option allows users to clear any applied filters and revert to the default state of the group list. It helps users start a fresh search or remove any unintended filters.
- **All Groups List**
  - In the CRM system, the Groups Management feature provides a comprehensive list of all groups created by the administrator. The list includes essential details for each group, such as:

- The Group Name
- The Date of Creation.

- Additionally, actions are available for administrators to perform on each group in the list. These actions typically include editing/updating the group and deleting it if necessary.

- **Edit/Update Group:**
  - When selecting the Edit/Update action for a group, administrators can modify various aspects of the group's configuration. The following options are commonly available for updating a group:
    - Update Group Name:
      - Administrators can modify the name of the group by entering a new value in the input field. This allows for changes to better reflect the purpose or attributes of the group.
    - Update Developer Name:
      - Similarly, administrators can update the developer name associated with the group by entering a new value in the input field. This field might be used for internal reference or identification purposes.
    - Update Users:
      - To add users to the group, administrators can utilize a Kanban-style interface. The interface consists of two columns:
        - All Users Column:
          - This column displays a list of all users created by the administrator. It provides an overview of the available users that can be added to the group.
        - The Selected Users column:
          - Administrators can drag and drop users from the All Users Column to the Selected Users Column. This action includes the selected users in the group.
        - Validation:
          - A validation is in place to [ensure that at least one user is added to the group]

- **Delete Group:**
  - The Delete action allows administrators to remove a group from the system. A validation process is implemented to confirm the deletion, ensuring that the action is deliberate and preventing the accidental removal of a group.

- **Add Group**
  - The CRM system includes an Add Group feature that allows administrators to create new groups within the platform. When adding a group, administrators are prompted to provide the following information:
    - **Group Name:**
      - Administrators enter the desired name for the group in the provided input field. This name serves as a unique identifier for the group.
    - **Developer Name:**
      - Similarly, administrators enter the developer name for the group in the input field. The developer's name may be used for internal reference or identification purposes.
    - **Update Users:**
      - To assign users to the newly created group, a Kanban-style interface is utilized. The interface consists of two columns:
        - **All Users Column:**
          - This column displays a list of all users created by the administrator. It provides an overview of the available users that can be added to the group.
        - **Selected Users Column:**
          - Administrators can drag and drop users from the All Users Column to the Selected Users Column. This action includes the selected users in the group.
        - **Validation:**
          - A validation is implemented to ensure that at least one user is added to the group before proceeding.
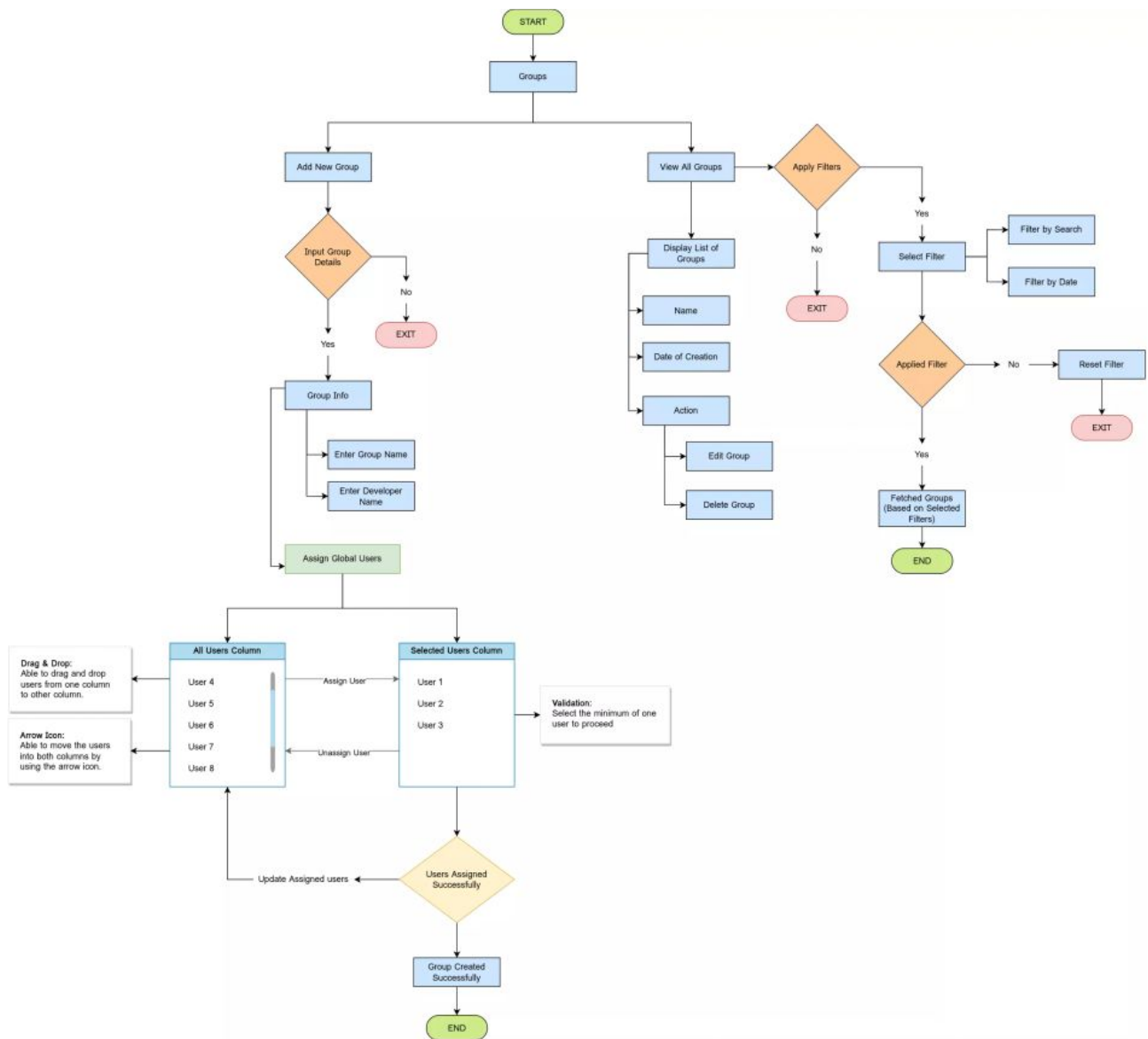
Userflow Diagram:

Group Management - User Flow Diagram

Settings

App Settings

In CRM, the App View feature allows administrators to manage and interact with different apps created within the platform. The feature provides a list of all the apps available in the system. Administrators have several actions they can perform on each app, including Edit, Clone, and Delete.

- **Apps View**
  - By utilizing the App View feature, administrators can efficiently manage the apps within the CRM system. They can edit app settings to customize functionality, clone apps for streamlined app creation, and delete apps when they are no longer needed. This enables administrators to effectively tailor the CRM platform to meet the specific requirements of their organization.
    - **List All Apps:**

      This feature in the CRM system provides administrators with an overview of all the apps available within the platform. It presents a comprehensive list of the apps that have been created and configured for use. The purpose of this feature is to provide

administrators with easy access to the apps and facilitate efficient app management. Each app is typically accompanied by three options that can be performed on the app. These options include:

- Edit App
- Clone App
- Delete App

- **App Creation:**
  - The creation of an app allows businesses to tailor their CRM system to their specific needs, enhancing productivity and efficiency in managing customer relationships and business processes. There are total of five basic steps to create an app within a CRM system, you can follow these basic steps:
    - **Step 1 (App Info)**
      - The first step in creating an app within the CRM system involves providing the necessary App Info. The System Administrator is required to fill in specific details in the input fields during this step. (* Indicates Required Fields)
        - App Name*
          - The System Administrator needs to enter a unique name for the app.
          - The System Administrator needs to enter the app name while considering the validation rules.
            - **Validation:** There is a validation rule that allows only alphabets, numbers, and underscores. Spaces and special characters are not permitted in the app name because the developer name will then be auto-generated based on the app name entered.
          - The chosen name serves as an essential identifier for the app within the CRM system. A well-chosen app name not only facilitates easy navigation and recognition but also provides users with a clear understanding of the app's role and significance.
        - Developers Name*
          - This field typically auto-generates based on the app name entered.
            - **Validation:** Only Alphabets and Numbers with underscore allowed no spaces
        - App Description (Optional)
          - The System Administrator is required to provide a short introductory description of the app. This description offers a brief overview of what the app is about and its main features or functionalities.
          - It helps to gain a quick understanding of the app's purpose and potential benefits.
        - App Image/Logo*
          - The System Administrator is required to upload an app image/logo. This serves as a visual representation of the app and helps administrators to easily locate and recognize the app, improving navigation and usability within the CRM system.
          - When the administrator uploads an image there is a button that is typically provided at the top corner of the image. This cross button serves as a delete or remove option for the uploaded image.
          - If the administrator wishes to delete the uploaded image and replace it with another image, they can simply click on the cross button. This action triggers the removal of the current image from the system.
          - To optimize response times, all images are stored in an S3 bucket. This setup ensures that when the system administrator adds or updates images, the retrieval process benefits from the efficient S3 infrastructure, leading to reduced response times. This approach enhances the overall performance of image-related operations by leveraging the S3's streamlined data storage and retrieval mechanisms.
      - User Flow Diagram
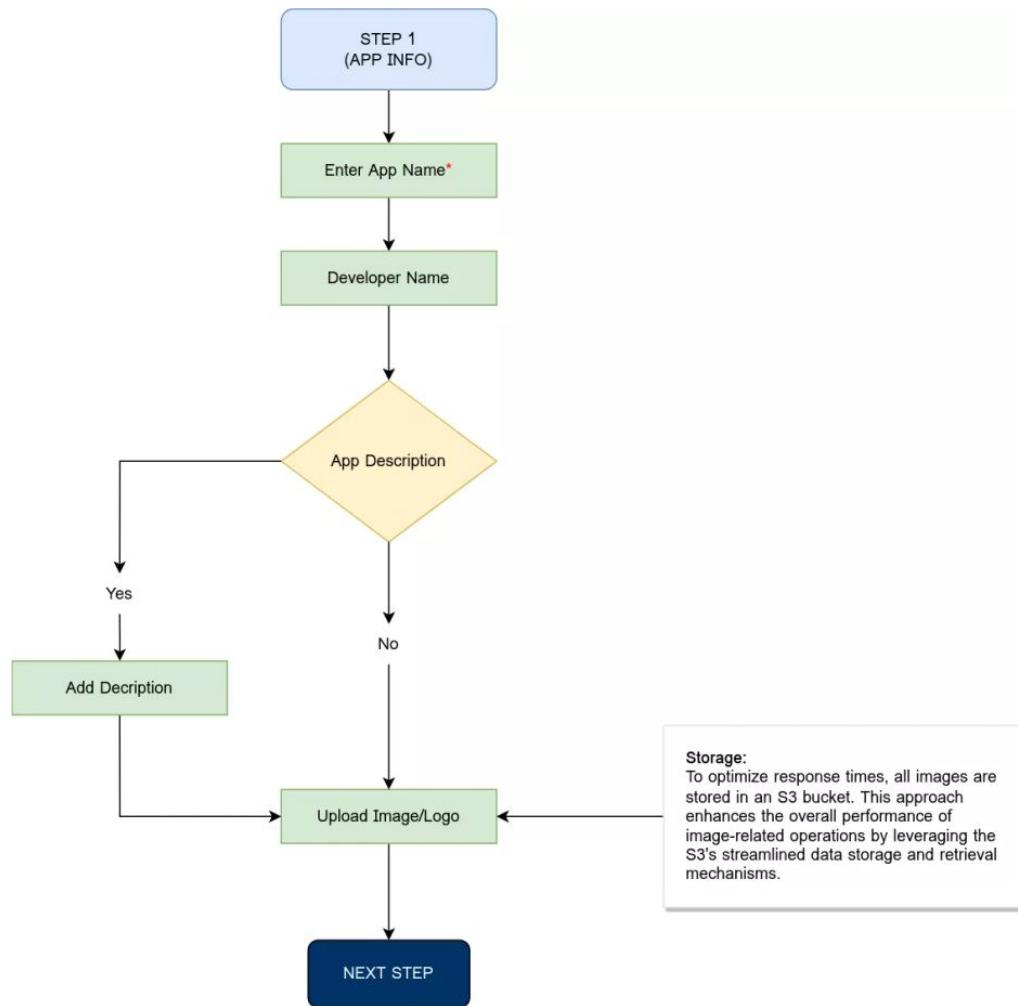
Step 01 - App Info

- **Step 2 (Global Profiles)**
  - The Administrator will be able to assign the profiles to the app in this step. The Global Profiles feature in the CRM system enables administrators to add the details and configurations of a new app, including the assignment of profiles. When creating an app, the Global Profiles feature provides a Kanban-style interface to manage and assign profiles to which that particular app would be visible and have the permissions based on that. The interface includes two columns:
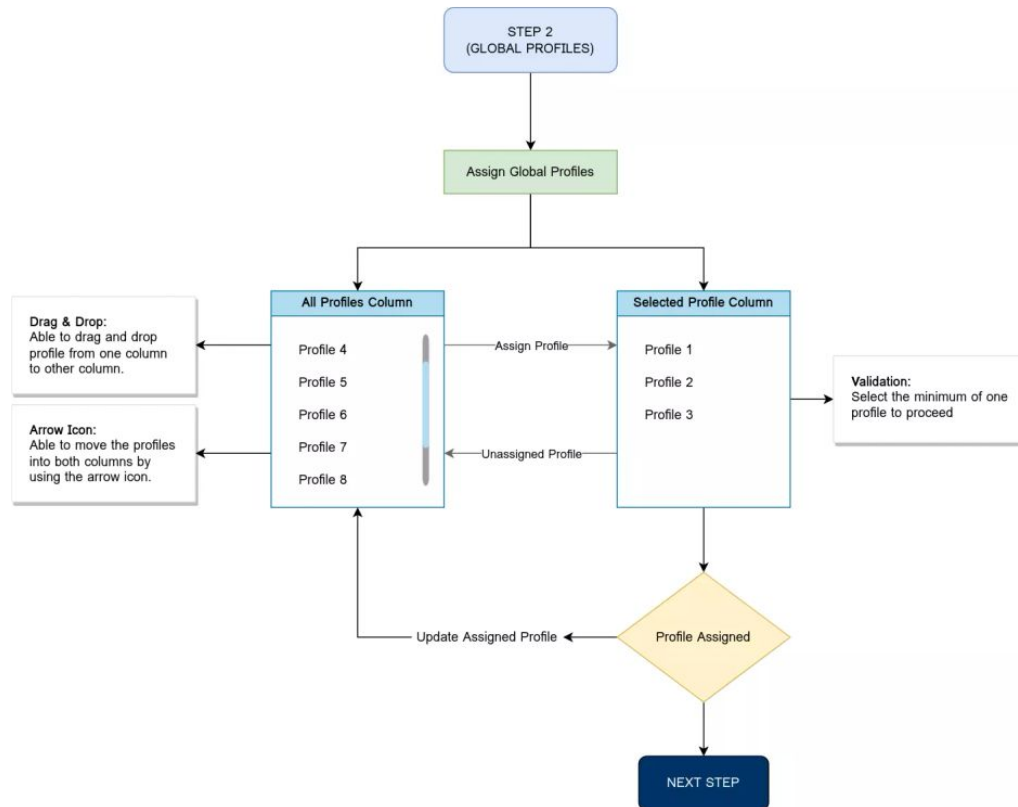   - **All Profiles Column:**
      - This column displays a comprehensive list of all the profiles available in the CRM system.
      - It allows administrators to review and select profiles that are relevant to the app being created.
      - The list provides an overview of the available profiles, ensuring that administrators have a comprehensive range of options to choose from.
      - Administrators can drag and drop the profiles from the All Profiles Column to the Selected Profiles Column.
      - Administrators can also move the profiles into the both columns respectively by using the right and left arrows present next to each profile as per the column in which the profile exists.
    - **Selected Profiles Column:**
      - By this the administrator can select the profiles that he wants to assign with that app.
      - Administrators can drag and drop the profiles from the All Profiles Column to the Selected Profiles Column.
      - Administrators can also move the profiles into the both columns respectively by using the right and left arrows present next to each profile as per the column in which the profile exists.
      - This action assigns the selected profiles to the app being created. The profiles listed in the Selected Profiles Column represent the profiles that are currently associated with the app.

- **Validation:** A validation is implemented to ensure that at least one profile is selected before proceeding.
  - <u>User Flow Diagram</u>

Step 02 - Global Profiles

- **Step 3 (Global Modules)**
  - This step of the app creation process allows administrators to add and manage modules within a specific app that is being created. Using a Kanban-style interface, administrators can easily select and add modules to the app. The Global Modules interface consists of two columns:
    - **All Modules Column:**
      - This column displays a comprehensive list of all available modules in the CRM system.
      - Administrators can review the list to identify the modules that are relevant to the app being created or updated. It provides an overview of the available modules, ensuring administrators have a wide range of options to choose from.
      - Administrators can also move the modules into the both columns respectively by using the right and left arrows present next to each profile as per the column in which the module exists.
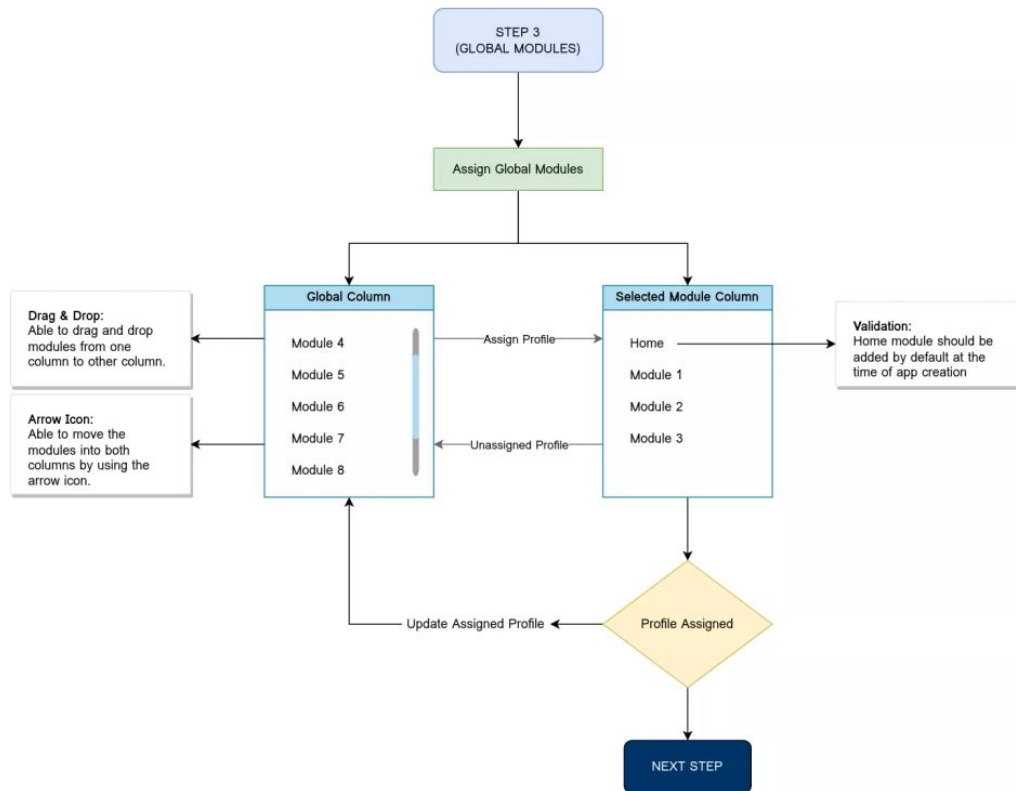   - **Selected Modules Column:**
      - Administrators can drag and drop modules from the All Modules Column to the Selected Modules Column.
      - Administrators can also move the modules into the both columns respectively by using the right and left arrows as per the column present next to each profile in which the module exists.
      - This action assigns the selected modules to the app, indicating that those modules are included in the app's functionality.
      - The Selected Modules Column displays the modules that have been selected for the app.
      - **Validation:** A validation is implemented to ensure that at least one module is selected before proceeding.
    - **Order Selection:**
      - System Administrators possess the ability to manage the display order of selected modules within the context of the app's edit mode. This is the same order for the modules followed when the system administrator sees these modules in the Edit Mode Screen.

- By transferring modules from the "All Modules" column to the "Selected Modules" column, administrators can establish a preferred order for the displayed modules.
- This process involves a straightforward drag-and-drop mechanism, enabling administrators to arrange modules as desired, specifying their positions, and enhancing the overall user experience of module navigation and interaction.
  - i.e System Administrator moves the three modules from the all Modules Columns to the Selected Module Column. Now he is able to change the order for the selected modules like which is on first place, second place and so on by simply just dragging the column to their respective place.
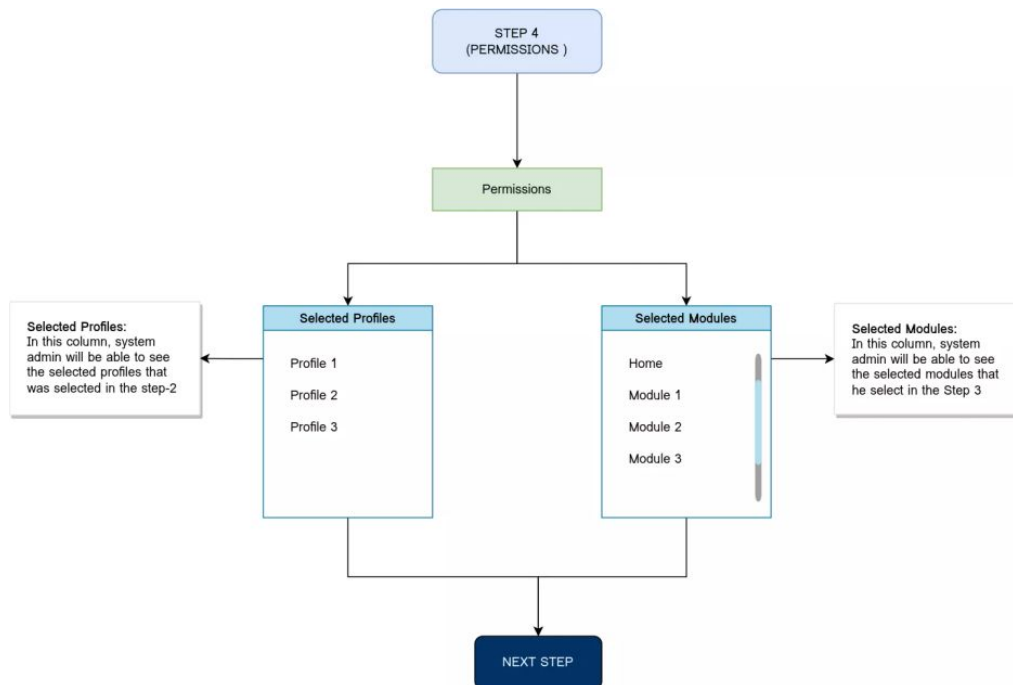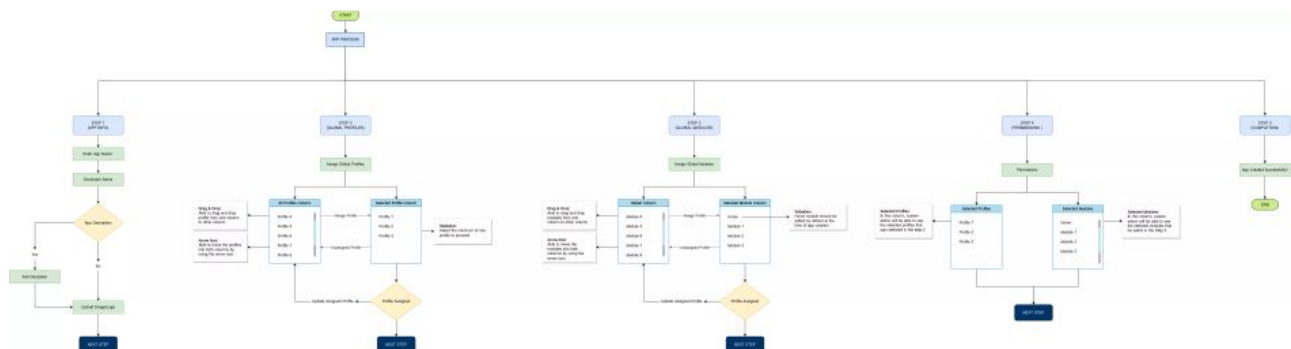 - User Flow Diagram

Step 03 - Global Modules

- **Step 4 (Permissions)**
  - In this step, the system administrator initially encounters a list of selected profiles within the "Selected Profiles" column alongside with the list of selected modules in the "Module" column.
  - User Flow Diagram:

Step 04 - Permissions Screen

- **Step 5 (Completion/Success):**
  - When the system administrator presses the complete button then the popup modal opens and a notification appears immediately after the app is successfully created, serving as visual feedback to the user.
- Userflow Diagram:

- **Edit App:**
  - This action enables administrators to modify the settings and configurations of a specific app. By selecting the Edit option, administrators can access and update various aspects of the app, such as:
    - **Step 1 (App Info)**
      - App Name
      - Developer Name
      - App Description
      - App Image
    - **Step 2 (Global Profiles)**
      - Modify, Update or Remove the Assigned Profiles
    - **Step 3 (Global Modules)**
      - Modify, Update or Remove the Assigned Modules.
    - **Step 4 (Permissions)**

- In this step, the system administrator initially encounters a list of selected profiles within the "Selected Profiles" column alongside with the list of selected modules in the "Module" column.
- Upon clicking on any specific profile, the system administrator is presented with a list of all modules associated with that profile.
- When a system administrator clicks on a module, it initiates an expansion revealing the View Types and Views linked to that module. Similarly, upon clicking on a View Type, the system administrator can further expand the list to display all the individual views that belong to that specific View Type.
- These Views are interactive when a system administrator clicks on a specific View, they are directed to the corresponding edit mode screen. This edit mode screen provides them with access to the relevant data associated with that particular View.

- **Clone App:**
  - Administrators can create a duplicate/clone of an existing app by selecting the Clone option. This functionality is useful when there is a need to create a similar app with similar configurations and settings as an existing one. The cloned app can then be customized further based on specific requirements.
    - **Validations:**
      - **Unique App/Developer Name:**
        - When the administrator attempts to clone any app along with its features & functionalities, the system should check if the App and developer name entered is unique. This can be done by comparing the inputted name with the existing developer names in the system.
        - If the name is already in use, an error message should be displayed, prompting the administrator to enter a different and unique developer name.
          - ***Error:*** *Developer name should be unique. This one already exists*
        - *As the developer name is automatically generated by the system based on the app name from which the system administrator wants to create an app. So, The App name must be unique.*
      - **Clone App Name:**
        - While cloning an app, The system automatically generates the app name at the time of cloning i.e App_clone.
        - Either it is not the required field to change the app name but the administrator has the option to change the app name. This allows for easier identification of the cloned app and distinguishes it from the original app. The system should provide a field or prompt where the administrator can enter a new name for the cloned app.
      - **Initiate the Clone Second Time:**
        - If the System Administrator wants to clone the app for a second time within the CRM system, they would need to manually input a unique app name. This is because the system typically generates a unique app name, such as "App_Clone," only once during the initial cloning process.
        - When initiating the second app cloning, the system does not automatically generate a new unique app name. Instead, the System Administrator must manually provide a distinct and unique name for the new cloned app. This ensures that each cloned app within the CRM system has a unique identifier and can be easily distinguished from other apps.
      - **Clone a Previously Cloned App:**
        - If the System Administrator wishes to clone a previously cloned app within the CRM system, the cloning process remains the same as for the app cloning. However, there is a consideration when it comes to naming the newly cloned app.
        - The system automatically generated a name for the cloned app i.e App_Clone_Clone.
      - **Cancel/Quit Cloning Operation:**
        - If the System Administrator initiates the App Clone feature within the CRM system but decides to abandon or cancel the operation at any step, the system will display a prompt confirmation message to ensure that they intended to quit the cloning process. This prompt aims to prevent accidental termination of the cloning operation and provides an opportunity for the administrator to confirm their decision.
        - The confirmation message may include a question such as "Are you sure you want to quit the cloning process?" or a similar inquiry to confirm the administrator's intention. The message serves as a precautionary measure to avoid any unintended consequences or data loss resulting from an incomplete or abandoned cloning operation.
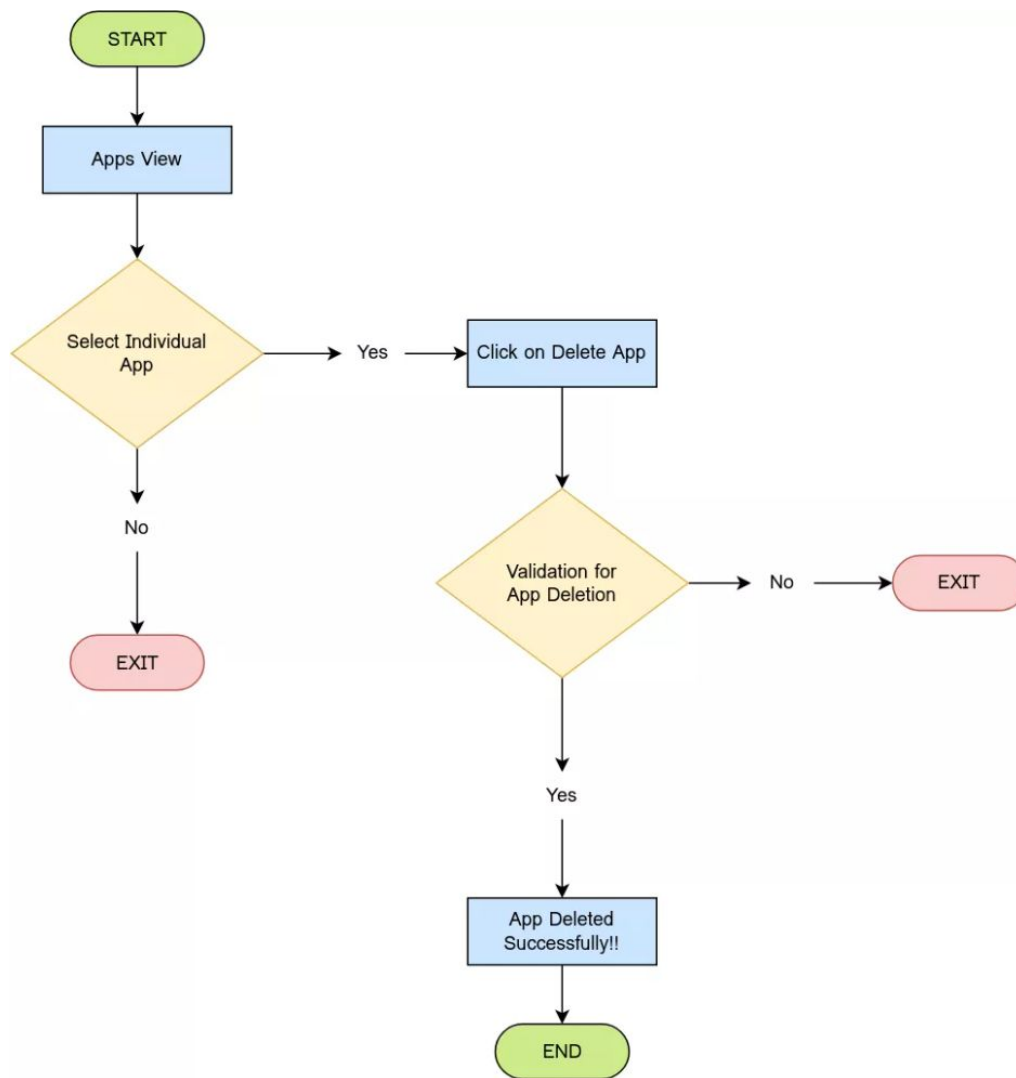
- <u>User Flow Diagram:</u>
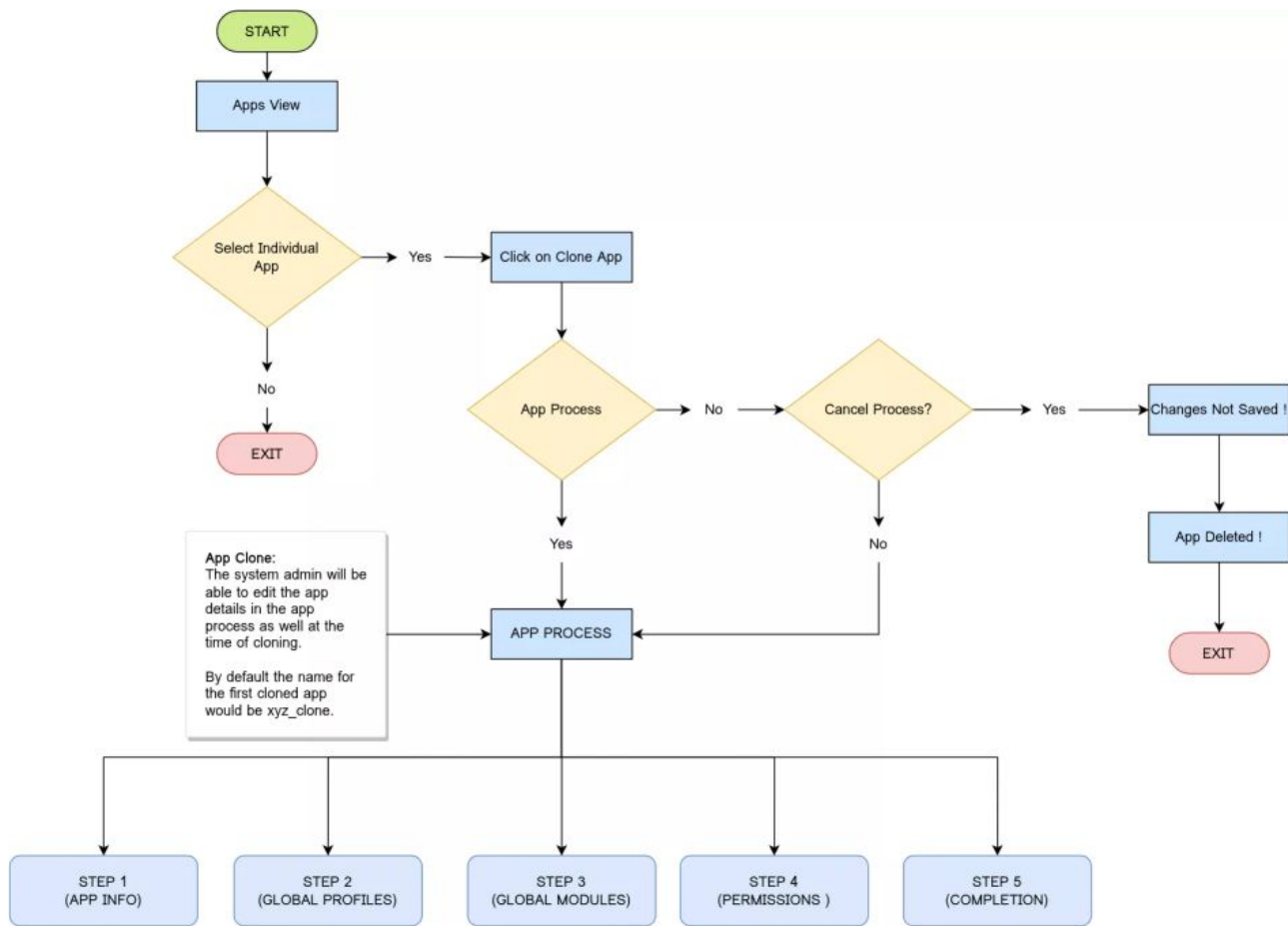
App Clone - User Flow Diagram

- **Delete App:**
  - The Delete option allows administrators to remove an app from the system. When this action is selected, a validation process is typically initiated to confirm the deletion. This ensures that the app is intentionally deleted and prevents accidental removal of an app.
  - <u>User Flow Diagram:</u>

Delete App Module - User Flow Diagram

Lead Mapping

Refers to the process of mapping or aligning the fields and data from a lead source or external system to the corresponding fields in the CRM system. It ensures that the data collected from various lead sources is accurately and seamlessly transferred into the CRM, allowing for efficient lead management and follow-up.

During lead mapping, administrators or users configure the mapping rules or settings to define how the data fields from the lead source should be mapped to the corresponding fields in the CRM. This mapping is typically based on field names, data formats, and data types.

- Modules
  - Lead Fields w.r.t Module Fields

Web to Lead

- To create a lead through a web form, CRM utilizes a lead generation feature that allows you to design and deploy a web form on your website. This web form serves as a mechanism for website visitors to submit their information and express their interest in your products or services.
- The process typically involves the following steps:
  - **Creating a new lead form:**
    - In the CRM if a system administrator looks for an option or feature that allows them to create a new lead form or web form. Click on it to initiate the form creation process.

- **Selecting fields for the form:**
  - Choose the specific fields you want to include on the lead form. These fields capture the necessary information from the users who submit the form. Common fields may include name, email address, phone number, company name, job title, country, city and many other relevant data fields. When users initiate or create a web form, they will typically encounter a two-column layout that displays the available fields on one side and the selected fields on the other side. This layout allows users to easily customize the form by choosing which fields to include.
    - **Available Fields:**
      - The "Available Fields" column showcases a list of fields that can be added to the web form. These fields are typically provided by the CRM system and can include various types of fields such as name, email address, phone number, company name, job title, country, city and many other relevant data fields. Users can browse through this column to find the specific fields they want to include in the form.
    - **Selected Fields:**
      - On the other side, the "Selected Fields" column displays the fields that have been chosen by the user to be included in the web form. Users can drag and drop or use a selection mechanism to move fields from the "Available Fields" column to the "Selected Fields" column. As fields are selected, they will appear in the "Selected Fields" column in the order they were added.
  - **Specifying the return URL:**
    - Determine the specific URL where users will be redirected after submitting the lead form. This is typically a "thank you" page or any other destination on your website that acknowledges their submission and provides relevant information or instructions.
  - **Generate the form:**
    - After configuring the form settings, save your changes and click on the Generate button. After That, You are able to publish the form to make it live and accessible on your website.
  - **Embedding the form on your website:**
    - Obtain the embed code provided by the CRM system for the lead form. This code can be inserted into the HTML of your website's pages or shared as a hyperlink on appropriate landing pages or contact sections to capture the leads.

By creating a lead through a web form, you establish a streamlined process for capturing and managing potential leads directly within your CRM system. This enables effective lead tracking, engagement, and conversion, facilitating the growth of your business.

App Dashboard & Edit Mode

App Dashboard

Clicking on "Apps" from the side menu triggers a drop-down list to appear. This list contains all the available apps within the profile. From this list, the administrator chooses the specific app they wish to access by simply clicking on its name. As a result, the dashboard for the selected app opens up, granting the administrator access to all the features and functionalities associated with that particular app.

- **Individual App Dashboard**
  - In the Dashboard, the system administrator can access a comprehensive view of all assigned modules along with their respective lead details data, when the Edit Mode toggle button is not enabled.
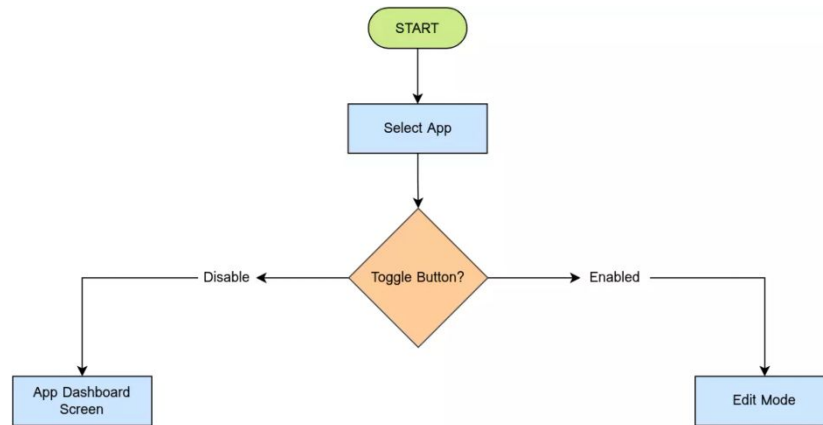   - **Modules**
      - Those modules are displayed here that system administrators select at the time of app creation.
      - The modules are pre-added to the system at the time of app creation and accessible within the app i.e Lead, Company, Contact & Opportunity.
      - The modules are organized in accordance with the order specified by the System Administrator during the app creation process. This sequence ensures that the modules are displayed systematically, aligning with the administrator's intended arrangement for easy access and efficient management within the CRM platform.
      - Upon selecting a specific module tab, the System Administrator gains access to a list of lead details. Within this view, he can access and manage the following details,
        - **Search Bar**

- A convenient search feature that enables quick and targeted searches based on specific lead details or criteria.
  - **Filters**
    - Customizable filters that allow the System Administrator to refine the displayed lead details based on different parameters, enhancing data visibility and analysis.
  - **Lead Detail List**
    - First Name
    - Last Name
  - Lead Status
    - New
    - Open
    - Closed
    - Contacted
    - Not Contacted
    - Converted
  - **Action:** Various action options that the System Administrator can take for each lead, including:
    - **Call:** Allows them to initiate a call directly from the CRM, streamlining communication with leads.
    - **View Lead Details:** Provides a comprehensive view of all lead information, facilitating a comprehensive understanding of their status and interactions.
    - **Edit Lead Details:** Enables the System Administrator to update and modify lead details as required, ensuring accurate and up-to-date information.
    - **Delete:** Offers the option for System Administrator to remove a lead from the CRM, aiding in lead management and data organization.
  - **Add Lead**
    - **First Name:** In Lead Details, "First Name" refers to the given name or forename of a potential customer or lead. It represents the individual's personal identification, usually provided at the time of lead addition by the system administrator.
    - **Last Name:** In Lead Details, "Last Name" refers to the family name, surname, or "second name" of a potential customer or lead.

Edit Mode

System Administrator will be able to enter the Edit mode option by clicking on the app from the dropdown list in the side menu and enabling the edit mode option from the toggle button that is present on the top right corner.

The main dashboard view in the edit mode provides system admin with a comprehensive view of all the modules, view types etc that are associated with the selected app. It serves as a centralized hub where system admin can access and manage the various details within the app.

The System Administrator has the ability to view all assigned modules associated with an app on the first tab associated with the app. This tab provides an overview of the modules that are currently assigned to the app.

The system administrator will be able to create the new module from this section as well associated with the profiles. Within this module tab the system administrator will be able to see and manage the following data,

- **Modules Order Sequence**
  - The modules are organized in accordance with the order specified by the System Administrator during the app creation process. This sequence ensures that the modules are displayed systematically, aligning with the administrator's intended arrangement for easy access and efficient management within the CRM platform.
- **Add Module**
  - To add a new module, system admin can utilize the "Add Module" functionality. The System Administrator can create a new module by following these steps:
  - Click on the "Add Module" button, typically located at the end of the modules tab interface.
  - Enter the Module Name in the Input Field, which serves as the identifier for the new module.
  - Once the system administrator enters the module name, the next step involves assigning the appropriate profile to that specific module. To facilitate this, the system presents a dropdown list containing all the profiles that were selected during the initial creation process of the app. Also, the system administrator can assign multiple profiles to one module as well.
  - Upon clicking the "Save" button after configuring the module details, a success popup will promptly appear. This popup serves as a confirmation that the module has been successfully integrated into the CRM system under the designated app.
  - When a new module is created, it is automatically positioned at the end of the list in the "All Modules" tab.
- Furthermore, modules are often associated with different view types and views. These represent different ways of displaying and interacting with the data within the module. By default, any newly created module has its own default view type, default view that is auto-generated by the system.

User-Flow Diagram:
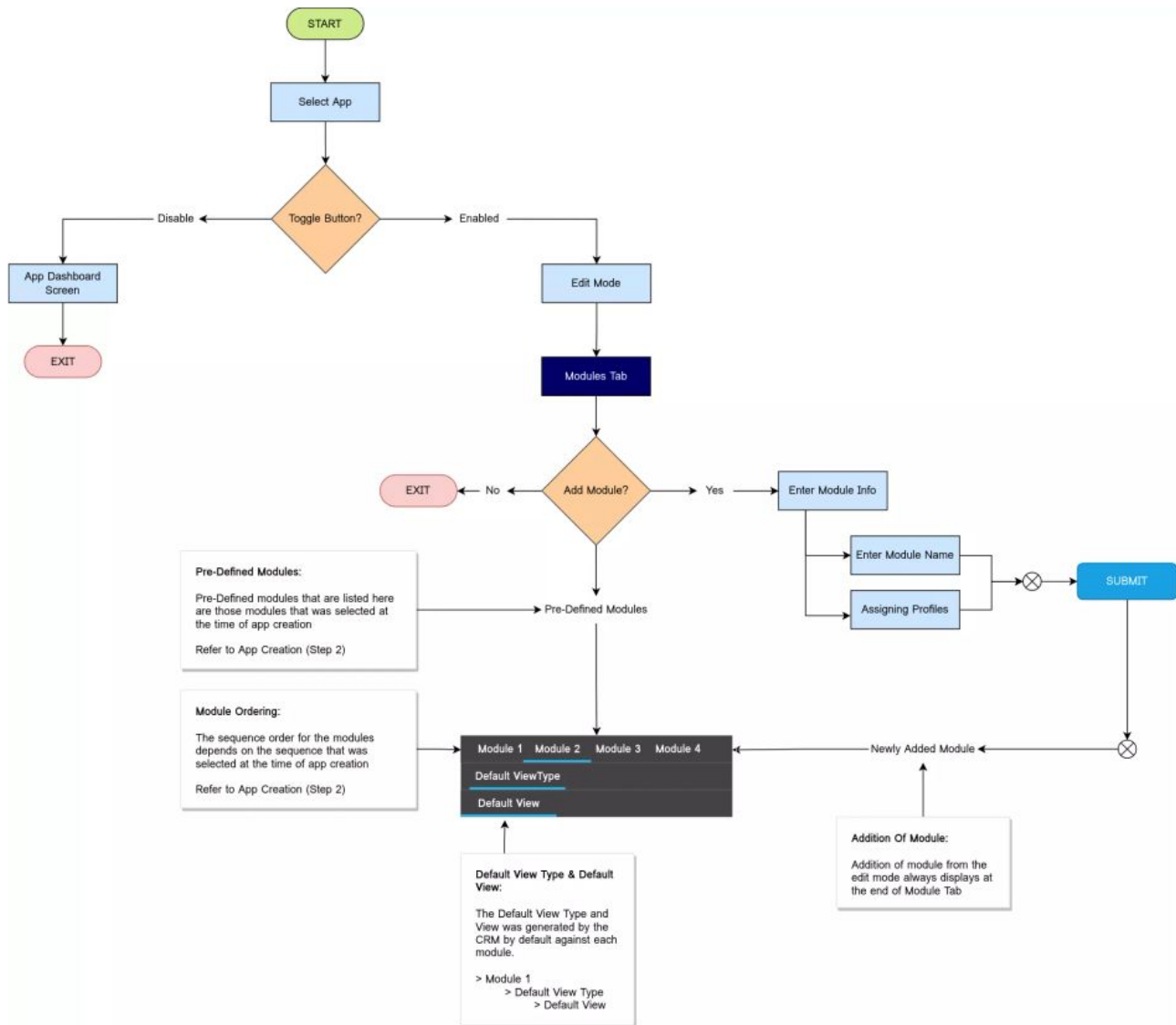
Edit Mode | Modules - User Flow Diagram

View Type

The System Administrator has the ability to manage views to define view types based on the selected modules and roles, ensuring that each module shows relevant information in a format that suits their needs. The second tab within the associated app is dedicated to managing view types related to specific modules. Here are the key points to understand about view types within the app:

- **List of View Types**
  - The second tab in the Edit Mode displays a list of all the view types created for the associated app. Each view type is typically associated with a specific module, allowing system admin to organize and view data in different ways within that module.
- **Creation of Multiple View Types**
  - The System Administrator has the ability to create multiple view types associated within the selected module. This enables customization and flexibility in displaying data based on different criteria, filters, or sorting preferences.
- **View Type Addition:**
  - When creating a new view type, a modal window typically appears to prompt the System Administrator to specify which view type they want to add.
  - In that modal, the system admin can simply write a name of View Type in the input field.
  - After entering the name, the system admin presses the save button. This ensures that the view type is correctly associated w.r.t the module and allows for seamless management and organization of view types within the app.
  - When a new view type is created, it is automatically positioned at the end of the list in the "All View Type" tab.

- **Profile Association**
  - Profiles can be added to multiple view types within the app. This means that the System Administrator can assign the same profiles to different view types, allowing them to access and interact with the corresponding data based on their permissions and privileges.

User Flow Diagram
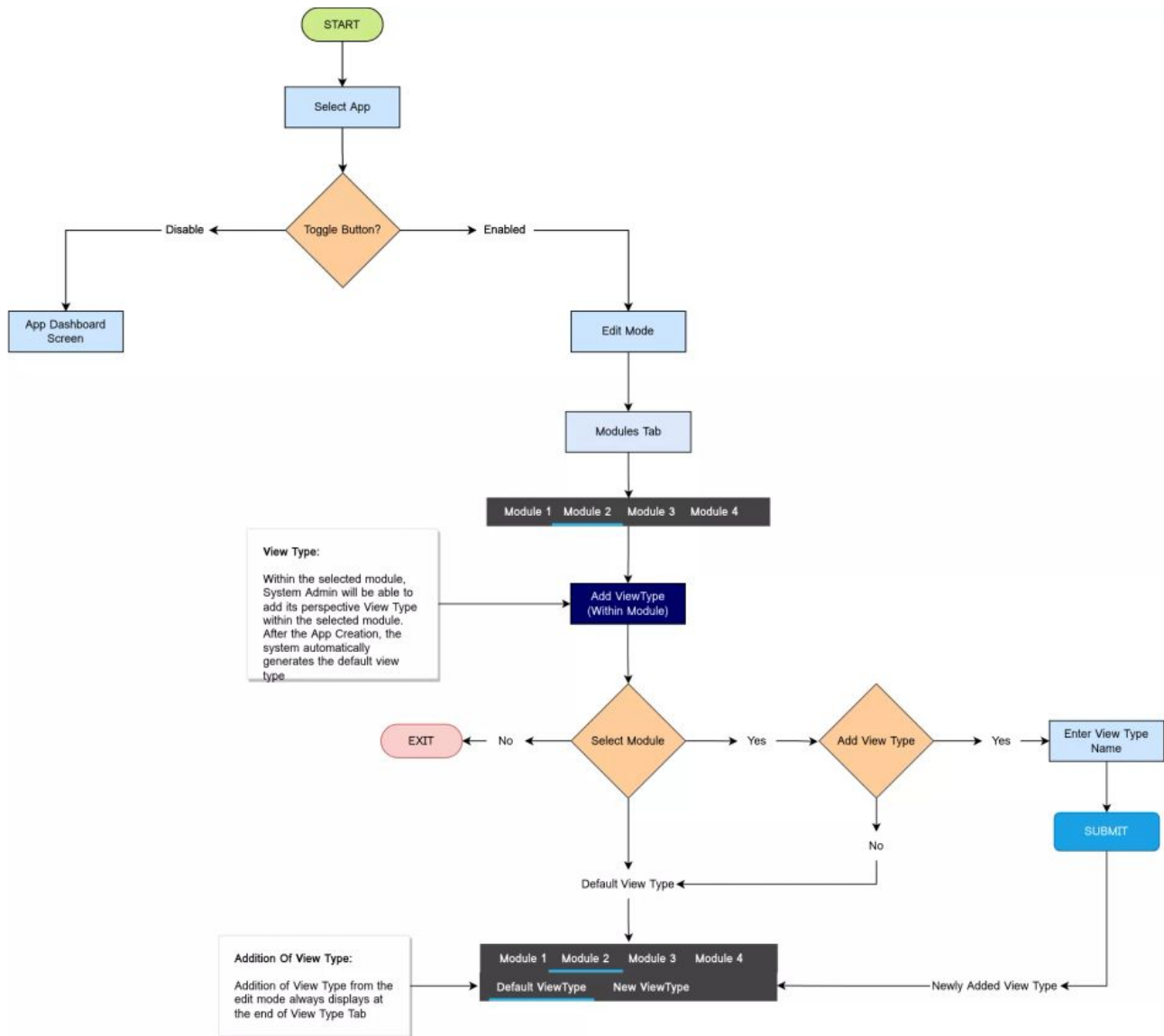
Edit Mode | View Type - User Flow Diagram

Views

The System Administrator has the ability to manage views associated with the selected view type and module.

- **Default View:**
  - When a System Administrator creates a new module, the CRM system automatically generates the default View Type and a default view specifically for that module.
  - The default view represents the initial arrangement or presentation of data for users accessing that view type and module.
- **Creating New View:**
  - Additionally, the System Administrator can create multiple custom views associated with the selected view type and module. These custom views allow for different arrangements, sorting options, filters, and data display configurations tailored to specific needs or workflows.
  - When the System Administrator is creating a new view within the CRM system, they will follow these steps:

- **Add View**
  - The system admin will need to select the View Type in which he wants to create an view
- **Enter View Name***
  - Once the Master View (View Type) is selected, the System Administrator needs to click on "Add View".
  - By doing so, they will be prompted to provide a name for the new view in a modal window.
  - This name will help identify the view and distinguish it from other views within the same view type.
- **Select Master View (View Type)***
  - In the field for selecting the master view, a dropdown menu displays a list of all previously created views. This dropdown is primarily used for cloning purposes.
  - However, when the System Administrator is creating a new view from scratch, they can leave this field blank as it won't be applicable in this context.
- **Clone View***
  - When the system administrator needs to clone an existing view within an specific view type then he needs to click on the "Add view" button
  - After selecting "Add View," the System Administrator needs to choose the existing view that he wants to clone from the dropdown menu.
  - The dropdown menu typically contains the list of available view types that have been defined for the selected module. It serves the purpose of facilitating cloning operations.
  - After submitting the save button, the cloned view has been successfully created.
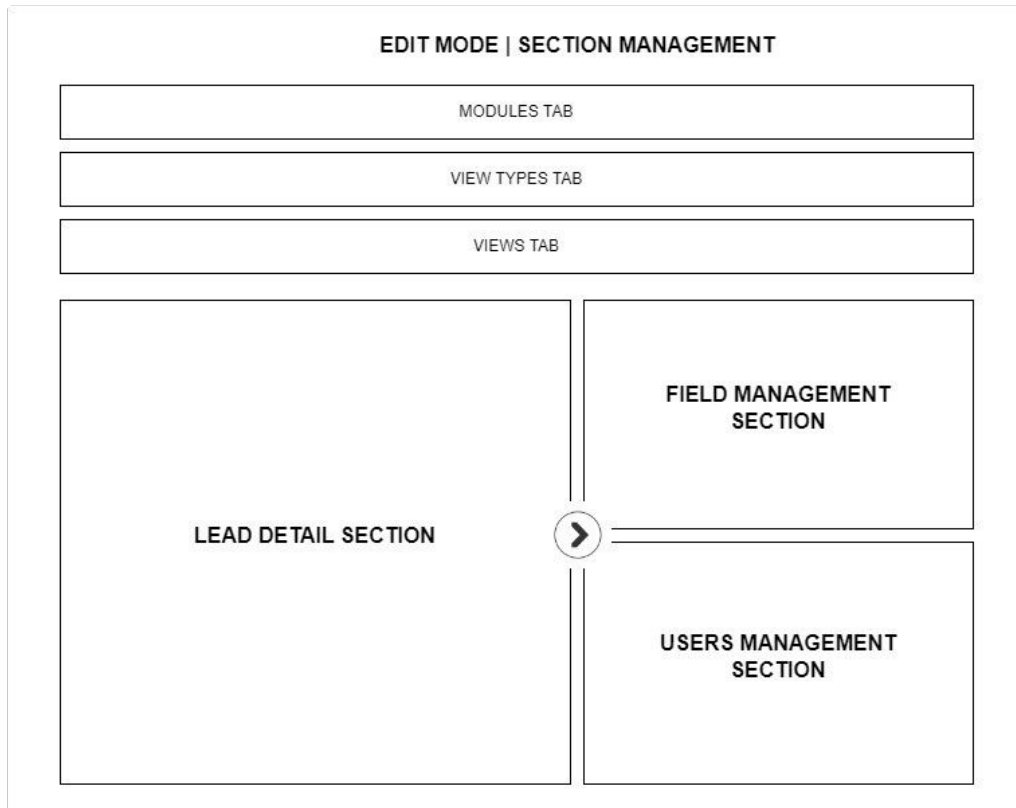
Section Management

The System administrator will be able to view or set the sections within the view for the specific profile associated with the selected view, view type and modules. When the System Administrator adds a new section, the process will involve the following steps:

- **New Section**
  - The System Administrator clicks on the "New Section" button to initiate the creation of a new section.
- **Enter Section Name**
  - After clicking on the "New Section" button, a modal or input field will appear where the System Administrator can enter the name of the new section in the provided input field.
- **Success Popup**
  - Once the System Administrator successfully enters the section name and clicks on the appropriate confirmation button, a success popup will be displayed, confirming that the new section has been added. The popup may display a message such as "Successful Section Addition."
- **Drag and Drop Fields**
  - With the new section now created, the System Administrator can proceed to drag and drop fields into the newly added section. This allows the System Administrator to organize and arrange the fields as needed within the section.
- **Placement of New Section**
  - The newly added section will be placed under the "Lead Details" section and will appear underneath any previously existing sections. This hierarchical structure helps organize and present the data in a clear and user-friendly manner.
- **Adding Multiple Sections**
  - The System Administrator can add multiple sections within the selected view. This feature allows them to customize the view's layout and structure according to the requirements of the specific profile or the nature of the data being displayed.
- **Section Customization**
  - For each added section, the System Administrator can customize it further by dragging and dropping fields into the section. This enables them to organize and arrange the data fields in a manner that best meets the requirements.

There is a useful feature that allows for expandable and collapsible screens within views. This feature provides flexibility in managing the visibility and organization of sections, enhancing the user experience

- **Expandable/Collapsible Screens**
  - There should be an option to collapse or expand screens using an arrow icon. For instance, if the admin desires to focus solely on the view types and lead details, they can simply click on the arrow icon. As a result, the right section of Field/User Management will collapse, and the admin will have an unobstructed view of the expanded view section.

Field Management

The System Administrator has the ability to manage and add fields from the section. This feature empowers the System Administrator to customize and organize the data fields within the section to best suit the needs of the specific profile, view, view type, and modules. By default, The field management consist of the three main components that includes,

- **Field Info**
  - In this particular section, The system administrator will be able to add the field info like field name, placeholder, label, control type etc
    - **New Field**
      - When the System Administrator wants to add a new field then he needs to click on the "New Field" button.
      - Upon clicking on the "New Field", the "Field Info" section will be automatically opened by default. Rest of the fields are:
        - Field Label
        - Field Name
        - Placeholder Text
        - Field Control Types (Dropdown)
        - Checkboxes
      - Upon opening the Field Info section, the cursor will be automatically placed in the field label input field by default. This will enhance the user experience and streamline the creation process.
    - **Success Popup**
      - After the System Administrator enters all the details into the field info section, a success popup appears, confirming the successful addition of the field. The success popup typically contains a brief message or notification that highlights the successful action taken by the System Administrator.
    - **Newly Added Fields**

- When the System Administrator adds new fields to a section, by default, these newly added fields are placed in the "Not Visible to Layout" section. This default placement helps to prevent the fields from immediately appearing on the user interface until the system admin decides to show these fields to the users/profiles.
    - The "Not Visible to Layout" section acts as a staging area for newly added fields, keeping them hidden from the user interface until the System Administrator decides to make them visible by placing them in the appropriate sections or layouts.
      - **Module-Fields Linking (One-To-Many Relationship)**
        - If the administrator wants to use the fields of the other modules within any existing module then he must select the relationship and select the module at the time of field creation.
        - By doing that he will be able to build the relationship and see the fields later in the Global Fields section (i.e if the system administrator stands in Lead Module and wants to use the fields of Contact Module)

- **Field Visibility**
  - In this section, The system administrator will be able to manage the permissions using the Checkboxes against the all profiles, users and groups that are associated with the app w.r.t the view of which the administrator wants to manage the permissions. The interface allows for collapsible/expandable sections to efficiently organize the information.

- **All Profiles (Collapsible/Expandable Screen):**
  - Under the "All Profiles" section, the system administrator can view and manage permissions for each profile (i.e Profile 1, Profile 2, Profile 3) against the corresponding view names. The "Read" and "Edit" access options are displayed against each profile name and the system can manage the permissions for each profile using the checkboxes.

PROFILES	READ ACCESS	EDIT ACCESS
Profile 1	☐	☑
Profile 2	☐	☑
Profile 3	☑	☐

- **All Groups (Collapsible/Expandable Screen):**
  - Similarly, Under the "All Groups" the system administrator can view and manage permissions for each group (i.e Group 1, Group 2, Group 3) against the corresponding view names. The "Read" and "Edit" access options are displayed against each group name and the system admin can manage the permissions using checkboxes.

GROUPS	READ ACCESS	EDIT ACCESS
Group 1	☑ -	☑ -
Group 2	☐ -	☑ -
Group 3	☑ -	☐ -

- **All Users (Collapsible/Expandable Screen):**
  - Under the "All Users" the system administrator can view and manage permissions for each User (i.e User 1, User 2, User 3) against the corresponding view names. The "Read" and "Edit" access options are displayed against each user name and the system admin can manage the permissions for each user using checkboxes.Under the "All Users" the system administrator can view and manage permissions for each User (i.e User 1, User 2, User 3) against the corresponding view names. The "Read" and "Edit" access options are displayed against each user name and the system admin can manage the permissions for each user using checkboxes.

USERS	READ ACCESS	EDIT ACCESS
User 1	☑ -	☑ -
User 2	☐ -	☑ -
User 3	☑ -	☐ -

- **Field Management (Existing Fields) :** There are two subsections that are associated with this particular section,
  - **Not Visible on Layout:**
    - When a system administrator adds a new field it will automatically be shown in this section.
    - System Administrator would be able to drag and drop the fields into the "Lead Details" section.
    - There would be a Search bar in this section with an input field by which the system administrator can search the leads that are added over time
  - **Global Fields (Related Fields):**
    - In this section, The system administrator would be able to see all the fields that are associated with each module and the fields that are interlinked globally between two modules. i.e. If the System Administrator builds the relationship between the Opportunity Module & Company Module then Company Module fields are also shown in the global fields within the Opportunity Module.
    - There would also be a Search bar in this section with an input field by which the system administrator can search the global fields.

User Management

In the User Management module, the system admin will have the ability to manage user profiles, groups, and individual users using checkboxes for easy selection and management. The following options are available.

The System administrator can view the below-mentioned details in the access management

- Profiles
  - All the Profiles will be listed here with the check box which those checkboxes will be true whose added while creating the profile.
  - The System administrator will be able to select more profiles to give them access to that particular Module, View Type and View which was selected.
  - The system administrator will be able to see all the users by clicking on a specific profile.
    - The system will show the list of all users along with the checkboxes
    - If the System Administrator wants to remove any specific user from that particular app then he must uncheck the checkbox.
      - **Validation:** When an administrator attempts to remove a specific user from that particular app, a validation prompt is displayed to ensure confirmation of the action. The purpose of this validation prompt is to prevent the accidental deletion of users and to provide an extra layer of caution before proceeding with the removal.
- Groups
  - All the groups will be listed here
  - The System administrator will be able to see the list of all group members by clicking on the group name.
  - The system administrator chooses or deselects options by clicking on the checkbox.
- Users
  - All the user's list will be listed here except
    - Those who are already in the profile.
  - The System administrator will be able to select the users by clicking on the checkbox.
    - System Administrator will also be able to remove the users by deselecting the checkbox. This will remove the user from that particular app.