Name: Tawer A. Kidanu

Atomic Requirements for Membership Management System

Purpose:

This document outlines the atomic requirements for a Membership Management System that supports membership creation, visit tracking, notifications, reporting, and user authentication and access control. It provides clear, testable, and prioritised requirements, definitions of key terms, scope of the system, and a glossary of terms. The requirements are designed to be self-contained, specific, and free of ambiguity.

Summary of Stakeholders

- **Primary Users:** Club Members
- **Operational Stakeholders:** Club Managers, Front Desk Staff
- **Technical Stakeholders:** IT Administrators, Software Development Team
- **Strategic Stakeholders:** Club Owners/Stakeholders, Legal/Compliance Team

Each stakeholder plays a key role in ensuring the system functions properly and meets its intended goals, balancing user experience, security, and operational efficiency.

Atomic Requirements

Requirement 1: **Membership**

1.1 Membership Creation

Importance: Essential
Description:

The system shall allow club staff to create a new membership by entering the following details:

- Member Name (First name and Last name)
- Contact Information (Phone number and Email address)
- Membership Duration (Options: 6 months, 1 year, 3 years)
- Upfront Membership Fee

Conditions:

- Membership is not created if any of the fields are left blank.
- The system will display a confirmation page showing the entered details before final submission.
- The system must check if the member's email or phone number is already associated with an active or recently expired membership. If such a record exists, the system should prompt the staff to either proceed with a renewal or deny the new membership creation.

- The system must validate the format of the phone number and email address before accepting them, ensuring that they meet standard formatting guidelines.
- Membership creation shall be reversible within a 24-hour period, allowing staff to cancel the membership if necessary, but only if no transactions have occurred related to that membership.
-The Membership cancellation request shall be logged with the reason and timestamp for audit purposes.
- The system should provide staff with feedback on the membership creation process, indicating success or failure clearly and allowing for immediate correction of any errors.
- The membership fee must be validated against a predefined list of valid amounts, ensuring that incorrect values are rejected.

Testable Condition:

- Upon entering valid details, the system successfully creates a membership and stores it in the database.
- If mandatory fields are left blank, the system prompts an error message.
- If the cancellation of a membership is requested within 24 hours, the system successfully removes the membership from active status without any related transactions.

1.2 Membership ID Assignment

Importance: Essential
Description:

Upon successful creation of a membership, the system shall automatically assign a unique membership ID to each member. This ID can be printed as a physical membership card or accessed through a mobile phone.

Conditions:

- The membership ID is a 10-digit unique number.
- The membership ID should not be generated until all the necessary steps in Requirement 1 are satisfied.
- The system must validate that the generated membership ID follows the predefined format.
- The ID can be scanned at check-in via a barcode on the membership card or QR code via the mobile app.
- If the membership ID cannot be generated for any reason (e.g., system error), an error message must be displayed, and the staff must have the ability to retry the generation process.

Testable Condition:

- The system generates a unique membership ID for every new membership, which can be validated as distinct from any existing ID.

1.3 Membership Expiration Tracking
Importance: Essential

Description:

The system shall track membership expiration dates and notify members when they check in if their membership has expired.

Conditions:

- Membership expiration is based on the duration selected at membership creation (6 months, 1 year, 3 years).
- Upon expiration, members must not be allowed to access club facilities without renewing.
- The system shall allow a grace period of up to 7 days after expiration, during which the member can still check in, but with a warning message stating that the membership has expired and needs to be renewed.
- All attempts to check in with an expired membership must be logged, including the date, time, and location of the check-in attempt for audit purposes.
- The system must generate daily reports for club staff, listing all memberships that have expired within the last 30 days and have not been renewed.

Testable Condition:
- The system should flag expired memberships during the check-in process and notify the member.

1.4 Membership Renewal
Importance: Essential
Description:

The system shall allow members to renew their membership either online or at the club reception upon expiration. The renewal duration and fee must match the previous membership period.

Conditions:
- Members cannot renew for a different duration than the original membership.
- Members must also be able to select a different membership duration during the renewal process if they choose to upgrade or downgrade.
- Payment of the renewal fee must be confirmed for membership to be extended.
- When a member renews their membership, the new expiration date shall extend from the current expiration date, not from the date of renewal (if the membership has not yet expired).
- If a member had a promotional discount on their previous membership, the renewal fee should reflect the standard price unless a new promotion is active.
- Upon successful renewal, the system shall immediately update the member's status to reflect the active membership.
- The member's mobile app or membership card (if applicable) should automatically reflect the new membership details.
- Members should have the option to enrol in **automatic renewal**, where the system automatically renews their membership using saved payment information.
- The system must allow for refunds or partial refunds in cases where a member renews but subsequently cancels within a designated period (e.g., 14 days after renewal).

Testable Condition:
- The system allows a member to renew their membership and confirms the extension with the same membership ID.

Requirement 2: Members Check-in Status

2.1 Check-In Process
Importance: Essential
Description:

The system shall allow members to check in by scanning their physical membership card or using the QR code on the mobile app. The system verifies the membership status at the point of check-in.

Conditions:
- The system must support multiple check-in methods, including:
    - Scanning a physical membership card with a barcode or RFID.
    - Scanning a digital membership card stored on a mobile phone via QR code, NFC, or other supported technologies.
- Membership must be valid at the time of check-in.
- Upon scanning, the system must immediately check if the member's membership is valid by comparing the current date with the membership's expiration date.
- The system must also check for any suspensions, freezes, or other restrictions on the member's account and prevent access if such conditions exist.
- Invalid or expired memberships trigger a notification and prevent check-in.
- The system must prevent members from checking in more than once within a short period (e.g., within 5 minutes) to avoid false data or abuse of the check-in system.

Testable Condition:
- The system accurately verifies membership validity and allows or denies check-in accordingly.

2.2 Visit Recording
Importance: Essential
Description:

The system shall record each member's visit when they check in, capturing the date, time, and membership ID for reporting purposes.

Conditions
- The system must automatically log each member's check-in, capturing member details, date, time, and check-in method.
- All visit data must include exact timestamps and be adjusted for time zone differences and daylight saving changes.
- The system must handle multiple check-ins per day as separate entries, avoiding duplicates within a short time window.

- Visit records must specify the facility visited, allowing multiple facility check-ins during a single visit.
- Members must be able to access their visit history, including details of visits over the last 12 months.
- The system must store visit data for at least 3 years and allow archived access to inactive members' records.
- Visit data must integrate with reporting systems, providing insights on attendance, frequency, and facility usage.
- Manual visit corrections by staff must be logged with a reason, staff name, and timestamp, ensuring accountability.

Testable Condition:
- The system stores the visit details and can retrieve them in reports.

2.3 : Invalid Membership Notification
Importance: Essential
Description:

The system shall notify members if their membership has expired or is invalid when they attempt to check in.

Conditions
- The system must notify members if their membership has expired upon attempting check-in.
- Notifications must be displayed immediately on the check-in screen before completing the process.
- The system must generate notifications if the membership is suspended or flagged for any other reason.
- Notification messages must be clear, providing reasons for invalid membership and steps for resolution.
- Members must be notified both on the check-in device and via email or SMS if their membership is invalid.
- The system must record all invalid membership attempts, including timestamps, for auditing and tracking purposes.
- The notification must include a direct prompt to renew the membership or contact customer service for support.
- Invalid membership notifications must remain visible until the member either renews or acknowledges the issue.

Testable Condition:
- Expired or invalid memberships trigger a pop-up or email notification.

Requirement 3: Report Generation
3.1 Frequent User Report Generation
Importance: Important
Description:

The system shall generate a report listing the most frequent visitors to the club based on a selected time range.

Condition

- The report must display the top users based on their number of visits in the chosen period.
- The system must provide options to filter the report by specific time ranges (e.g., weekly, monthly, quarterly).
- The system must allow staff to export the frequent user report in formats such as CSV or PDF.
- The report must include key details like member name, membership ID, and total number of visits.
- The system must allow staff to sort the report by visit count or alphabetically by member name.
- The system must provide visual indicators, such as bar charts or graphs, to highlight the top frequent visitors.
- The frequent user report must be accessible only to authorised staff members with proper role-based permissions.

Testable Condition:
- The system generates accurate reports of members based on visit frequency.

Requirement 4: Role-Based Access Control (RBAC)
Importance: Essential
Description:

The system shall implement role-based access control to manage user access. Club managers, staff, and IT administrators should have different levels of access based on their role.

Conditions:

- The system must implement role-based access control to manage user permissions effectively.
- Different user roles (e.g., club managers, front desk staff, IT administrators) must have distinct access levels based on their responsibilities.
- Club managers must have full access to all system features and data.
- Front desk staff must be able to check members in and view membership statuses but not access billing information.
- IT administrators must have the ability to manage system settings without accessing sensitive member data.
- The system must allow for easy modification of user roles and permissions by authorised personnel.
- Access control changes must be logged for audit purposes, including user ID, timestamp, and nature of the change.
- The system must provide an interface for users to view their assigned roles and permissions for transparency.

Testable Condition:
- The system restricts features based on user roles during login.

Requirement 5: Secure Login
Importance: Essential

Description:

The system shall require secure login credentials (username and password) for both staff and members to access sensitive information.

Conditions:
- The system must require all users (staff and members) to log in using secure credentials (username and password).
- Passwords must be stored using strong encryption techniques to ensure security.
- The system must enforce a minimum password complexity, requiring at least one uppercase letter, one lowercase letter, one number, and one special character.
- Users must be prompted to change their password every 90 days to maintain security.
- The system must implement a mechanism for password recovery, allowing users to reset their passwords securely.
- Login attempts must be limited to five consecutive failures before temporarily locking the account to prevent brute-force attacks.
- The system must log all login attempts, including successful and failed attempts, for security auditing.
- Users must receive a notification (via email or SMS) after a successful login from a new device or location for added security.

Testable Condition:
- The system successfully encrypts passwords and enforces secure login rules.

What if Scenarios ???

1- What if the member's email address has been previously entered but the phone number is new?
2- What if the member wishes to upgrade their membership type after initial submission but before payment?
3- What if the member loses their physical membership card but still has the ID?
4- What if the system fails to verify a valid membership?

Glossary

1. User: Any person (staff or member) who interacts with the system.
2. Membership ID: A unique identifier assigned to each member upon registration.
3. Check-in: The process by which a member enters the club by verifying their membership.
4. Proration: The calculation of partial membership fees based on the duration of use.
5. Role-Based Access Control (RBAC): A system that grants different access levels to users based on their role within the organisation.

6. Stakeholders : Individuals or groups who have an interest in or are affected by the system.
7. Primary Users: Individuals who directly interact with the system to achieve their personal or professional goals, such as club members utilising membership features.
8. Operational Stakeholders: Individuals responsible for the day-to-day management and operations of the system, ensuring it runs smoothly and meets user needs, such as club managers and front desk staff.
9. Technical Stakeholders: Individuals focused on the technical aspects of the system, including its performance, security, and maintenance, such as IT administrators and software development teams.
10. Strategic Stakeholders: Individuals involved in shaping the long-term vision and strategic direction of the system, ensuring it aligns with the organisation's overall goals and objectives, such as club owners and compliance teams.

Attributes

- Membership ID: 10-digit unique number assigned to each member.
- Member Name: String (First Name and Last Name).
- Membership Duration: List (6 months, 1 year, 3 years).
- Check-In Time: DateTime (records the time a member checks in).
- Prorated Fee: Decimal (calculated based on partial membership use).
- User Role: List (Club Manager, Front Desk Staff, IT Administrator).