Use Case: Logging in with an Existing Account

Iteration: 1, Initial version.

Primary actor: User (Returning Player)

Goal in context:

- To allow returning users to log in and access their OMG platform account.

Preconditions:

- The user has already registered and verified their account.
- The user has access to a web browser or application to log in.

Trigger:

- The user wants to log in to their existing account.

Scenario:

1. The user navigates to the OMG platform's login page.
2. The system displays a login form requesting:
   - Username or email
   - Password
3. The user enters their credentials and submits the form.
4. The system validates the credentials against stored user data.
5. If validation is successful, the system authenticates the user and grants access.
6. The system redirects the user to their dashboard, displaying their profile and game history.
7. If enabled, the system checks for saved preferences and applies them (e.g., dark mode, notifications).

Exceptions:

1. Incorrect username/email or password—system displays an error and prompts the user to try again.
2. Multiple failed login attempts—system may trigger a CAPTCHA or temporarily lock the account.
3. Forgotten password—user can request a password reset via email.
4. Account not verified—system prompts the user to verify their email before logging in.
5. System maintenance—if the platform is under maintenance, a message is displayed with an estimated availability time.

Priority: High priority, required for user access.

When available: First increment.

Frequency of use: Frequent.

Channel to actor: Via web browser or application.

Secondary actors:

- System administrator (for account recovery issues).
- Customer support (for troubleshooting login problems).

Channels to secondary actors:

- System administration dashboard.
- Customer support ticket system.

Open issues:

1. Should the platform support social media logins (Google, Facebook, etc.)?
2. Will two-factor authentication (2FA) be required or optional for enhanced security?
3. How long should login sessions remain active before requiring reauthentication?
4. Should the system notify users of login attempts from new devices or locations?