|  |  |  |  |
| --- | --- | --- | --- |
| ID and Name: | **UC02 - Login** | | |
| Created By: | nguyen cong manh | Date Created: | 11/10/24 |
| Primary Actor: | Student/Faculty | Secondary Actors: | none |
| Description: | This use case allows users to log into the system to access the functions of the online library. | | |
| Trigger: | Admin clicks on the "Login" button in main page. | | |
| Preconditions: | PRE-1. The user has an existing registered account in the system.. | | |
| Postconditions: | POST-1. The user is redirected to the main page of the system after a successful login | | |
| Normal Flow: | **2.0 Login**   1. The **user** accesses the **Login** page. 2. The **user** enters their email address and password. 3. The **user** clicks the **Login** button. 4. The **system** validates the login information. 5. If the information is valid:   The **system** redirects the user to the main page.   1. If the information is invalid:   The **system** displays an error message and prompts the user to re-enter their credentials. | | |
| Alternative Flows: | **2.1: Forgot Password**:   * If the user clicks on the **Forgot Password** link:   + The **system** redirects the user to the password recovery page. | | |
| Exceptions: | **2.0.E1 Invalid Credentials:**   * If the user enters incorrect email or password, the system displays an error message indicating the credentials are invalid and allows the user to try again.   **2.0.E2 Account Locked:**   * If the user exceeds the maximum number of login attempts, the account is temporarily locked. The system informs the user to contact support or wait a specified period to try again. | | |
| Priority: | High | | |
| Frequency of Use: | Daily, when users need to access the system. | | |
| Business Rules: | **BR-01:** Users must enter valid credentials (registered email and password) to access their accounts.  **BR-02:** The system must lock accounts after a predefined number of failed login attempts to enhance security. | | |
| Other Information: | 1. The login process should be implemented with secure protocols (e.g., HTTPS) to protect user data. 2. The system should log all login attempts for security auditing. | | |
| Assumptions: | 1. Users have internet access to log into the system. 2. Users remember their registered email and password for login.. | | |

A diagram of a network

Description automatically generated

A diagram of a library system

Description automatically generated

A diagram of a flowchart

Description automatically generated

A blue square with black text

Description automatically generated

A diagram of a network

Description automatically generated