**Backend API Technical Requirement Document**

**BOOKS MANAGEMENT SYSTEM – LOGIN API**

**1. Overview**

This document outlines the requirements for creating backend API endpoints to handle user authentication for the Books Management System.

**2. Objective**

* Develop API endpoints for user login.
* Implement validation for user credentials.
* Integrate the backend with the database to authenticate users.

**3. Success Criteria**

* API returns a success response upon valid user authentication.
* API returns an error response upon invalid user credentials.
* User authentication is securely managed.
* Authenticated users receive appropriate access tokens for further API requests.

**4. Endpoints**

* **POST /api/auth/login**
  + **Purpose:** Authenticate user credentials.
  + **Request Body:**

Json { "username": "string", "password": "string" }

* + **Response:**
    - Success (HTTP 200 OK):

Json { "success": true, "message": "Login successful", "accessToken": "string" }

* + - Error (HTTP 401 Unauthorized):

Json { "success": false, "message": "Invalid username or password" }

**5. Error Handling**

* Invalid username or password: Return HTTP 401 Unauthorized status code with an appropriate error message.
* Server errors: Return HTTP 500 Internal Server Error status code with an error message.

**6. Authentication**

* Use a secure authentication method such as JWT (JSON Web Tokens) to generate and verify access tokens.
* Verify user credentials against a database of registered users.
* Ensure passwords are securely hashed before storing them in the database.