**API Documentation – Loan Management System**

**Base URL**

The LMS system will be hosted in two environments:

1. Production - Live system for real users. https://api.yourdomain.com
2. Staging - For testing without affecting live data. https://staging.yourdomain.com/api

**Authentication**: Bearer Token (JWT)

Every request needs a JWT token (login token) to prove the user is authorized.

**Authentication Endpoints**

These allow people to register and log in. After login, they get a token used for all future API calls.

1. POST /auth/register

Registers a new user.

Request Body

{

"full\_name": "Eric Kisu Nzuma",

"email": "kisueric4@gmail.com",

"password": "securePassword123"

}

Response

{

"message": "User registered successfully",

"userId": 1

}

1. POST /auth/login

Authenticates a user and returns a JWT token.

Request Body

{

"email": "kisueric4@gmail.com",

"password": "securePassword123"

}

Response

{

"token": "jwt\_token\_string"

}

**User Management**

Only admins can view or edit users.

Regular users (borrowers) can't access these endpoints.

GET /users

Returns a list of all users (Admin only).

GET /users/:id

Returns the profile of a specific user.

PUT /users/:id

Updates a user’s profile (Admin only).

DELETE /users/:id

Deactivates a user account (Admin only).

**Loan Management**

Borrowers apply for loans.

Admins review and approve or reject.

Status updates trigger notifications.

POST /loans

Submits a new loan application.

Request Body

{

"amount": 10000,

"duration\_months": 12,

"interest\_rate": 5.0

}

GET /loans

Retrieves all loan applications (Admin only).

GET /loans/:id

Retrieves the details of a specific loan.

PUT /loans/:id/approve

Approves or rejects a loan.

Request Body

{

"status": "approved",

"admin\_comment": "Approved based on creditworthiness."

}

**Repayment Management**

Borrowers use this to repay loans (via M-Pesa).

Tracks when, how much, and how it was paid.

POST /repayments

Records a loan repayment.

Request Body

{

"loan\_id": 1,

"amount\_paid": 2000,

"payment\_method": "mpesa"

}

GET /repayments/:loanId

Retrieves all repayments for a specific loan.

**Notifications**

These endpoints allow users to check reminders, approvals, and messages from the system.

Admin or system can mark them as read.

GET /notifications

Fetches notifications for the authenticated user.

PUT /notifications/:id/read

Marks a specific notification as read.

**Audit Logs**

Admin-only view of all system actions (for security & tracking).

GET /audit-logs

Retrieves a list of system activity logs (Admin only).

**External API Integrations**

These are automatic system-to-system connections. The user doesn’t manually trigger them.

* Credit Scoring API (via TransUnion)

Used to fetch a user's credit score during loan application evaluation.

Example Endpoint Consumed:

POST /external/credit-score

Request Body

{

"user\_id": 1,

"national\_id": "12345678"

}

Response

{

"credit\_score": 720,

"risk\_level": "Low"

}

* M-Pesa STK Push:

Prompts borrower’s phone to pay for a loan.

Endpoints Consumed

POST /external/mpesa/stkpush

{

"phone\_number": "254712345678",

"amount": 2000,

"transaction\_type": "loan\_repayment"

}

* M-Pesa B2C

Sends loan money to user’s phone after successful application.

POST /external/mpesa/b2c

{

"phone\_number": "254712345678",

"amount": 10000,

"purpose": "loan\_disbursement"

}

* Twilio/SendGrid

Sends reminders/status updates by SMS or email.

POST /external/notify

{

"recipient": "kisueric4@gmail.com",

"message": "Your loan has been approved."

}

Response

{

"status": "sent"

}

**Error Format**

Any time something goes wrong (e.g., invalid password), the system responds in this standard format so developers can handle it cleanly. All errors follow a consistent format.

{

"error": "Unauthorized access",

"status": 401

}

**Access Control Table**

This shows who can do what.

|  |  |  |
| --- | --- | --- |
| **Endpoint** | **Borrower** | **Admin** |
| /auth/\* | yes | yes |
| /loans (POST) | yes | no |
| /loans (GET) | no | yes |
| /repayments | yes | yes |
| /users | no | yes |
| /notifications | yes | yes |
| /audit-logs | no | yes |
| /external/\* | no | yes |