Academic Management System - API Documentation

Phase 1: Authentication & Authorization

1. Register User

Description: Creates a new user in the database with a securely hashed password and assigned role.

- **Endpoint URL:** /auth/register
- **HTTP Method:** POST
- **Required Headers:** Content-Type: application/json
- **Authentication Requirement:** No

Request Body Format:

```
{
    "full_name": "Nicole Lamoste",
    "email": "nicole@university.edu",
    "password": "mypassword123",
    "role_id": 1
}
```

Response Format (Success - 201):

```
{
    "message": "User registered successfully!"
}
```

Response Format (Error - 400 Bad Request):

```
{
    "error": "Email already exists"
}
```

2. Login User

Description: Authenticates a user using email and password, returning a secure JWT token for session management.

- **Endpoint URL:** /auth/login
- **HTTP Method:** POST
- **Required Headers:** Content-Type: application/json
- **Authentication Requirement:** No

Request Body Format:

```
{
    "email": "nicole@university.edu",
    "password": "mypassword123"
}
```

Response Format (Success - 200):

```
{
    "success": true,
    "message": "Login successful!",
```

"token": "eyJhbGciOiJIUzI1NiIsInR..."

}

Response Format (Error - 401 Unauthorized):

{

"error": "Invalid credentials"

}

3. Protected Profile Route

Description: A secure route that retrieves the logged-in user's profile information based on their JWT token.

- **Endpoint URL:** /auth/profile
- **HTTP Method:** GET
- **Required Headers:** Authorization: Bearer <JWT_TOKEN>
- **Authentication Requirement:** Yes

Request Body Format: *(None required)*

Response Format (Success - 200):

{

"message": "Welcome to your protected profile!",

"user": {

"id": 1,

"full_name": "Nicole Lamoste",

```
        "email": "nicole@university.edu",
        "role_id": 1,
        "created_at": "2026-02-24T14:25:02.000Z"
    }
}
```


Response Format (Error - 401 Unauthorized):


```
{
    "error": "Access denied. No token provided."
}
```


4. Admin Dashboard (RBAC Test)

Description: A role-restricted route that only allows users with an Admin role (role_id: 1) to access it.

- **Endpoint URL:** /admin/dashboard
- **HTTP Method:** GET
- **Required Headers:** Authorization: Bearer <JWT_TOKEN>
- **Authentication Requirement:** Yes (Must be Admin)

Request Body Format: *(None required)*

Response Format (Success - 200):


```
{
    "message": "Welcome Admin! You have special access to this route."
```

}

Response Format (Error - 403 Forbidden):

{

"error": "Access denied. Insufficient permissions."

}