# API Testing Checklist

## Authentication & User Management

☐ User Registration (POST /api/register/)

☐ Can Super Admin create new users?

☐ Can Admins or Basic Users register themselves? (They shouldn't)

☐ User Login (POST /api/login/)

☐ Can all users log in successfully?

☐ Does login return a valid token?

☐ User Permissions in Admin Panel

☐ Can Super Admins see and manage users?

☐ Can Admins log in but NOT manage users?

☐ Can Basic Users log in? (They shouldn't be able to)

☐ Token Authentication (Authorization: Token user\_token\_here)

☐ Does a valid token allow access to protected routes?

☐ Does an invalid token return 'Invalid Token'?

## File Management

☐ View Files (GET /api/files/)

☐ Can Basic Users see files?

☐ Can Admins see files?

☐ Does a user without a token get denied access?

☐ Download Files (GET /api/files/{id}/)

☐ Can Basic Users download files?

☐ Can Admins download files?

☐ Upload Files (POST /api/files/)

☐ Can Admins upload a file?

☐ Are Basic Users restricted from uploading?

☐ Edit Files (PUT/PATCH /api/files/{id}/)

☐ Can Admins edit file names?

☐ Are Basic Users restricted?

☐ Delete Files (DELETE /api/files/{id}/)

☐ Can Admins delete a file?

☐ Are Basic Users restricted?

## Project & Folder Structure

☐ View Projects (GET /api/projects/)

☐ Can all authenticated users see projects?

☐ Does filtering by constituency work?

☐ View Counties & Constituencies (GET /api/counties/ & /api/constituencies/)

☐ Can all authenticated users see them?

☐ View Files in a Project (GET /api/projects/{rfx\_number}/files/)

☐ Do files only show for the correct project?

## Security & Errors

☐ Unauthorized Access Tests

☐ Does a logged-out user get denied when accessing /api/files/?

☐ Does an invalid token cause 'Invalid token' error?

☐ Invalid Input Handling

☐ Does registering with an existing username return an error?

☐ Does uploading a file without a project ID return an error?

☐ Data Integrity

☐ Can users access only their allowed data?