File Encryption Tool – Epics, User Stories & Acceptance Criteria

# EPIC 1: User Authentication and Authorization

## User Registration

### Scenario: Successful user registration

* Given the user is on the registration page
* When the user enters a valid email and a strong password
* And submits the form
* Then the user should be registered successfully
* And a confirmation message should be displayed

### Scenario: Duplicate email error

* Given the user is on the registration page
* When the user enters an email that already exists
* Then an error message should be displayed saying "Email already registered"

## User Login

### Scenario: Successful login

* Given the user has a valid registered account
* When the user enters correct credentials
* Then the user should be redirected to the dashboard
* And receive a valid authentication token

### Scenario: Failed login

* Given the user is on the login page
* When the user enters incorrect credentials
* Then an error message should be displayed saying "Invalid email or password"

## Stay Logged In

### Scenario: Persistent login session

* Given the user has previously logged in and has a valid token
* When the user revisits the app
* Then the user should remain logged in
* And be redirected to the dashboard automatically

### Scenario: Token expired

* Given the token has expired
* When the user visits the app
* Then the user should be redirected to the login page
* And shown a message to log in again

## Forgot Password

### Scenario: Request password reset

* Given the user has forgotten their password
* When the user clicks on "Forgot Password"
* And enters their registered email
* Then a password reset link should be sent to their email

### Scenario: Reset password successfully

* Given the user clicks on a valid reset link
* When the user enters a new valid password
* Then their password should be updated
* And they should be redirected to the login page

# EPIC 2: File Encryption

## Upload File for Encryption

### Scenario: Upload valid file

* Given the user is on the encryption page
* When the user selects a supported file type
* Then the file should be accepted and shown in the UI

### Scenario: Upload invalid file

* Given the user selects an unsupported file type
* Then an error message should be shown

## Encrypt File with Password

### Scenario: Encrypt file successfully

* Given the user has uploaded a valid file
* And entered a strong password
* When the user clicks "Encrypt"
* Then the file should be encrypted
* And a success message should be shown

## Download Encrypted File

### Scenario: Provide download link

* Given the file is encrypted successfully
* When the process completes
* Then a download link should be shown to the user
* And the file should be downloadable

# EPIC 3: File Decryption

## Upload Encrypted File

### Scenario: Upload valid encrypted file

* Given the user is on the decryption page
* When the user uploads a previously encrypted file
* Then the file should be accepted for decryption

## Decrypt File with Password

### Scenario: Successful decryption

* Given the user has uploaded an encrypted file
* And entered the correct password
* When the user clicks "Decrypt"
* Then the file should be decrypted successfully
* And a success message should be shown

### Scenario: Incorrect password

* Given the user enters an incorrect password
* When the user tries to decrypt the file
* Then an error message should be shown stating "Incorrect password"

## Download Decrypted File

### Scenario: Provide decrypted file

* Given the file is successfully decrypted
* When the decryption completes
* Then the user should see a download link
* And be able to download the original file