Constraints

1. Authentication & Security

- The user must be authenticated (logged in).
- Token Requirement: A valid JWT token must be present in the.
- Session Validity: The provided token must be active and not expired.

2. Current Password Field

- Validation: The input must match the user's actual current password stored in the database (hash verification).
- Mandatory

3. New Password Field

- Length :Minimum of 8 characters.
- Complexity Requirements:
  - Must contain at least one lowercase letter
  - Must contain at least one uppercase letter
  - Must contain at least one digit
  - Must contain at least one special character
- The new password cannot be the same as the current password.

4. Confirm Password Field

- Mandatory.
- Consistency: Must match the New Password field exactly (case-sensitive).

Equivalence Class

1. Current Password Field

Class ID	Description	Type	Expected Result
CP1	Valid current password (matches DB)	Valid	Verified successfully.
CP2	Incorrect current password	Invalid	Error: "Incorrect current password."
CP3	Empty current password	Invalid	Error: "Please provide both current password and new password."
CP4	Whitespace-only current password	Invalid	Error: "Incorrect current password."

2. New Password Field

Class ID	Description	Type	Expected Result
NP1	Valid strong password (meets all criteria)	Valid	Accepted.
NP2	Valid minimum length (Exactly 8 chars)	Valid	Accepted.
NP3	Too short (< 8 characters)	Invalid	Error: "Password must be at least 8 characters."
NP4	Missing Uppercase letter	Invalid	Error: "Password must include uppercase..."
NP5	Missing Lowercase letter	Invalid	Error: "Password must include lowercase..."
NP6	Missing Digit	Invalid	Error: "Password must include a number..."

3. Confirm Password Field

Class ID	Description	Type	Expected Result
CFP1	Matches new password exactly	Valid	Accepted.
CFP2	Does not match new password	Invalid	Error: "New passwords do not match."
CFP3	Case-sensitive mismatch	Invalid	Error: "New passwords do not match."
CFP4	Empty confirm password	Invalid	Validation Error: Field is required.

4. Authentication & Authorization

Class ID	Description	Type	Expected Result
AUTH1	Valid JWT token (User logged in)	Valid	Authorized.
AUTH2	No token (User not logged in)	Invalid	Error: "You are not logged in. Please login again."
AUTH3	Expired or Invalid Token	Invalid	Error: "Unauthorized" / Redirect to Login.

Test cases

1. Current Password Validation

Test Case ID	Input	Equivalence Class	Expected Result
TC1	OldPass123! (correct)	CP1	Current password verified. Proceed to new password validation.
TC2	WrongPass123! (incorrect)	CP2	Error: "Incorrect current password." (401)
TC3	(empty field)	CP3	Error: "Please provide both current password and new password." (400)
TC4	" " (whitespace only)	CP4	Error: "Incorrect current password." (401)
TC5	" OldPass123! " (with spaces)	CP5	Error: "Incorrect current password." (401)

2. New & Confirm Password Validation

Test Case ID	**Input (Current / New / Confirm)**	**Equivalence Class**	**Expected Result**
TC6	[Correct Old] / NewPass123! / NewPass123!	NP1, CFP1	Password changed successfully.
TC7	[Correct Old] / Pass1! / Pass1! (7 chars)	NP3	Error: "Password must be at least 8 characters."
TC8	[Correct Old] / newpass123! / newpass123! (No uppercase)	NP4	Error: "Password must include uppercase, lowercase, number, and special character."
TC9	[Correct Old] / NEWPASS123! / NEWPASS123! (No lowercase)	NP5	Error: "Password must include uppercase, lowercase, number, and special character."
TC10	[Correct Old] / NewPass123 / NewPass123 (No special)	NP7	Error: "Password must include uppercase, lowercase, number, and special character."

TC11	OldPass123! / OldPass123! / OldPass123! (same as current)	NP9	Backend error: "New password must be different from your current password." (400)
TC12	[Correct Old] / NewPass123! / NewPass123!	CFP1	Passwords match. Proceed with change.
TC13	[Correct Old] / NewPass123! / DifferentPass123!	CFP2	Error: "New passwords do not match."
TC14	[Correct Old] / NewPass123! / newpass123! (case diff)	CFP3	Error: "New passwords do not match."
TC15	[Correct Old] / NewPass123! / "NewPass123! " (extra space)	CFP5	Error: "New passwords do not match."

3. Authentication & Authorization

Equivalence Class not applied here because it is applied to input fields that accepts variables

Test Case ID	Scenario	Input	Expected Result
TC16	User logged in with valid token	Valid JWT token	Authorized. Password change allowed.
TC17	User not logged in	Token is null	error: "You are not logged in. Please login again."
TC18	Invalid/malformed token	"invalid token123"	rejects (401 Unauthorized).
TC19	Expired JWT token	Expired token	rejects (401 Unauthorized).
TC20	User deleted after token issued	Valid token, user deleted	Backend error (404): "User not found."

`   4.Integration & User Flow

Equivalence Class not applied here because it is applied to input fields that accepts variables

Test Case ID	**Scenario**	**Input**
TC21	Complete Successful Flow	Current: OldPass123! / New: NewPass123!
TC22	Login after Change	Complete change flow
TC23	Old Password Check	After change, attempt login with old password
TC24	Concurrent Changes	Two sessions change password simultaneously
TC25	Backend Prevents Reuse	New password = current password