User Stories

**User Story 1: Multi-Factor Authentication (MFA)**

Role: Registered B2B user

Description:  
As a user of the platform, I want to make sure my login is secure. After entering my email and password, if MFA is enabled on my account, I should receive a 6-digit code by SMS or email to confirm it’s really me logging in.

Acceptance Criteria:  
- The system should check if MFA is enabled after validating the password.  
- If MFA is on, send a 6-digit one-time code (OTP).  
- The code should expire after 3 minutes.  
- Users can try entering the code up to 3 times.  
- If the code is correct → log the user in.  
- If not → show an error and redirect back to login.

Error States:  
- Expired code → 'The verification code has expired.'  
- Wrong code → 'Incorrect code. Please try again.'

Open Questions:  
- Are we supporting authenticator apps (e.g., Google Authenticator) or only SMS?  
- Should we allow users to generate backup codes?

**User Story 2: Password Recovery**

Role: Any user who forgot their password

Description:  
If a user forgets their password, they should be able to reset it easily by entering their email address. A reset link will be sent to their inbox, and they can use it to choose a new password.

Acceptance Criteria:  
- User enters their email address on the 'Forgot Password' screen.  
- If the email exists, send a reset link that expires in 30 minutes.  
- The user can set a new password (must be strong and at least 8 characters).  
- After updating the password, the user is redirected to the login page.

Error States:  
- Email not found → 'No account found with this email.'  
- Weak password → 'Password must be at least 8 characters long, including uppercase, lowercase, and a number.'

Open Questions:  
- Should we include a 'Confirm Password' field for extra safety?  
- Do we need a CAPTCHA to prevent bots from abusing the reset form?