Test Case Document
HopSkipDrive “Forgot Password”
Feature Prepared by: Anastasy Rogers
Date: 02/26/2025
Document Version: 1.0
App Version: 3.9.0-598

ID	Description:	Priority:	Precondition:	Steps:	Expected Result:	Actual Result:	Status (Pass/Fail):	Tester Initials:	Date Executed:	Defect ID:	App Version:
TC-FP-001	Verify that the “Forgot Password” link is accessible from the login screen	High	HopSkipDrive app is installed and launched	1. Navigate to the login screen 2. Look for “Forgot Password” or similar link/button	“Forgot Password” link/button is clearly visible and accessible on the login screen						
TC-FP-002	Verify that a registered email can be submitted through the forgot password flow	High	User has a registered account	1. Click on “Forgot Password” link 2. Enter valid registered email address 3. Submit the request	System accepts the email and shows confirmation message that reset instructions have been sent						
TC-FP-003	Verify that system validates email format	Medium	User is on the forgot password screen	1. Enter invalid email format(e.g., “test@test”, “test”, “test@.com”) 2. Submit the request	System displays appropriate error message indicating invalid email format						
TC-FP-004	Verify system behavior when non-registered email is entered	Medium	User is on the forgot password screen	1. Enter email address not registered in the system. 2. Submit the request	System should not indicate whether email exists or not (for security) but show a generic message about instructions being sent if account exists						
TC-FP-005	Verify that password reset email is delivered	High	Valid registered email has been submitted	1. Check email inbox (including spam/junk folders) 2. Verify email contains reset link and instructions	Reset email is received within a reasonable time (< 5 minutes)						
TC-FP-006	Verify that the password reset link in the email works correctly	High	Reset email has been received	1. Click on the reset link in the email. 2. Observe where the link directs to	Link opens app or browser to password reset screen						
TC-FP-007	Verify that new password validation works	High	User is on the password reset screen	1. Enter new password that doesn’t meet requirements (e.g., too short, no special characters) 2. Submit the form	System displays appropriate error message indicating password requirements						
TC-FP-008	Verify that password confirmation field is validated	Medium	User is on the password reset screen	1. Enter valid new password in the first field 2. Enter different password in the confirmation field 3. Submit the form	System displays error message indicating passwords do not match						
TC-FP-009	Verify that password can be successfully reset	High	User is on the password reset screen	1. Enter valid new password 2. Enter matching password in confirmation field 3. Submit the form	System confirms password has been reset and redirects to login screen						
TC-FP-010	Verify user can login with newly reset password	High	Password has been successfully reset	1. Navigate to login screen 2. Enter email and newly reset password 3. Submit login form	User successfully logs in to their account						
TC-FP-011	Verify that password reset link expires after a certain time	High	Reset email has been received, but not used for **24+** hours	1. Wait for at least **24** hours after receiving reset email 2. Click on the reset link in the email	Link is expired and displays appropriate message						
TC-FP-012	Verify system behavior when multiple reset requests are submitted	Medium	User has a registered account	1. Submit forgot password request for same email multiple times in succession	System handles multiple requests appropriately (either by sending multiple emails or by indicating that a request is already in progress)						
TC-FP-013	Verify integration with account lockout functionality	Medium	Account lockout policy is in place	1. Observe if there’s any limit to the number of password reset requests 2. Attempt to send multiple requests in a short period	System either limits the number of requests or has other protection mechanisms						
TC-FP-014	Verify UI elements are consistent with HopSkipDrive’s design system	Medium	Testing on mobile device	1. Navigate through entire forgot password flow 2. Observe UI elements, fonts, colors, spacing 3. Compare with other parts of the app (e.g., login screen) 4. Check that the HopSkipDrive logo and branding elements appear correctly	All UI elements maintain consistency with the rest of the app’s design system, with proper branding, spacing, and visual hierarchy						
TC-FP-016	Verify that error messages are clear and helpful	Medium	Testing various error scenarios	1. Trigger various error conditions 2. Observe error messages	Error messages are clear, specific, and provide guidance on how to resolve the issue						
TC-FP-017	Verify compatibility with screen readers for accessibility	Medium	Screen reader enabled on device	1. Navigate through forgot password flow with screen reader active 2. Verify all elements are properly announced	All UI elements are properly labeled and accessible via screen reader						
TC-FP-018	Verify system behavior when network connectivity is lost right as user submits email	High	User is in the forgot password flow	1. Enter email in forgot password screen 2. Turn off network connectivity (airplane mode) right before pressing submit 3. Press submit button 4. Observe system behavior 5. Turn network back on and verify if request is automatically retried or if user needs to resubmit	System shows appropriate network error message, preserves entered data, and allows retry once connection is restored						
TC-FP-019	Verify data persistence when switching between apps	Medium	User is on the new password entry screen	1. Begin entering new password 2. Switch to another app (e.g., email, messaging) 3. Return to HopSkipDrive app after **30** seconds 4. Observe if entered data is preserved	Partially entered data is preserved when returning to the app within a reasonable timeframe						
TC-FP-020	Verify application behavior when interrupted by incoming call	Medium	User is in the middle of password reset flow	1. Initiate password reset process 2. While on the new password screen, simulate incoming call 3. Answer call (or decline) and return to app 4. Observe application state	Application returns to same screen with data preserved after call interruption						
TC-FP-021	Verify timeout behavior after extended inactivity	Medium	User has started password reset process	1. Navigate to password reset screen 2. Leave application idle for at least **15** minutes 3. Return and attempt to continue	System either maintains state or shows timeout message with clear instructions to restart process						
TC-FP-022	Verify system handling of special characters in password	High	User is on new password entry screen	1. Try entering passwords with various special characters (**!@#$ %^~`&*()_-=+{}[]|\:;’,” <> ?/**) 2. Observe system behavior and validation messages	System accepts valid special characters and shows clear validation rules if certain characters are not allowed						
TC-FP-023	Verify password length limits are enforced	High	User is on new password entry screen	1. Try entering a very short password (**1-3** characters) 2. Try entering a very long password (**50+** characters) 3. Attempt to submit each	System enforces minimum and maximum length requirements with clear error messages						
TC-FP-024	Verify system handling of repeated character passwords	Medium	User is on new password entry screen	1. Try entering passwords with repeated characters (e.g., “aaaaaaa”, “111111111”, “ AAAAAAAA”) 2. Attempt to submit	System either accepts or rejects based on password complexity rules with clear messaging						
TC-FP-025	Verify system handling of non-Latin characters	Medium	User is on email or password entry screen	1. Enter email or password using non-Latin characters (e.g., Cyrillic, Chinese, Arabic, Polish, Emoji) 2. Attempt to submit	System either handles non-Latin characters appropriately or shows clear validation rules						
TC-FP-026	Verify proper navigation when using device back button	Medium	User is in the forgot password flow	1. Navigate to various screens in the forgot password flow 2. Press device back button at each step	Navigation works as expected, user can go back to previous screens without losing entered data						
TC-FP-027	Verify system behavior when device has low battery	Low	Device battery is below **10%**	1. Start password reset process on device with low battery 2. Observe any warnings or behavior changes 3. Complete reset process if possible	System completes process normally or gracefully handles any battery-related interruptions						
TC-FP-028	Verify system handling of unusual numerical email inputs	Medium	User is on forgot password email entry screen	1. Try entering email-like patterns with repetitive numbers (e.g., “111111@gmail.com”, “999999@gmail.com”) 2. Try entering email-like patterns with sequences (e.g., “12345@gmail.com”, “098765@gmail.com”) 3. Attempt to submit each	System validates email format correctly regardless of numeric patterns						
TC-FP-029	Verify system handling of common weak password patterns	High	User is on new password entry screen	1. Try entering commonly used weak passwords (e.g., “password123”, “qwerty”, “12345678”). 2. Try entering sequential keyboard patternsle.g., “qwertyuiop”, “asdfghjkl”) 3. Attempt to submit each	System enforces password strength requirements with clear feedback on what makes a strong password						
TC-FP-030	Verify copy-paste functionality for email and password fields	Medium	User is on email or password entry screen	1. Copy an email or password from another source 2. Attempt to paste into the respective field 3. Try to submit form with pasted content	Copy-paste functionality works properly, and pasted content is validated correctly						