| Title: Add Password Recovery | | | TaskID: 4567 | | |
| --- | --- | --- | --- | --- | --- |
| Current Workflow: User navigates to the login page of the system, typically through a web browser or mobile app.  User enters their username or email address, depending on the system's login requirements.  User enters their password, which is typically masked to prevent unauthorized access.  User clicks on the "login" button to submit the login information.  The system authenticates the user's credentials and verifies that the user is authorized to access the system.  If the login information is correct, the system redirects the user to the home page or dashboard of the system.  If the login information is incorrect, the system displays an error message and prompts the user to re-enter their login information.  Once the user is logged into the system, they can access the features and functions that are available to them based on their role and permissions.  When the user is done using the system, they can log out by clicking on the "logout" button or link, which ends the user's session and prevents unauthorized access to their account. | | | | | |
| Requirements: Forgot Password Link: Provide a "Forgot Password" link or button on the login page to allow users to initiate the password recovery process.  Verification Method: Provide a method for verifying the identity of the user, such as by sending a recovery link to the email address associated with the user's account or by asking security questions that only the user can answer.  User Information: Collect the user's information required for password recovery, such as the user's email address or username.  Password Reset Link: Generate a secure password reset link and send it to the user's email address or provide it on the recovery page.  Password Reset Process: Allow the user to reset their password by clicking on the secure password reset link and following the instructions to create a new password.  Password Complexity: Enforce password complexity rules to ensure that the user creates a strong and secure password that meets the system's password policy requirements.  Confirmation: Notify the user via email or on-screen confirmation message that their password has been reset successfully.  Account Lockout: Implement account lockout policies to prevent unauthorized access or abuse of the password recovery feature.  Security: Ensure that the password recovery feature is secure and cannot be exploited by hackers or malicious users to gain unauthorized access to user accounts.  Accessibility: Ensure that the password recovery feature is accessible to all users, including those with disabilities or who use assistive technologies. | | | | | |
| Expected Outcome: Improved User Experience: Users who forget their password will be able to recover it easily and securely, without having to contact support or create a new account.  Increased User Satisfaction: Users who are able to recover their password quickly and easily are more likely to have a positive experience with the system and to recommend it to others.  Reduced Support Costs: Providing a self-service password recovery feature can reduce the number of support tickets related to forgotten passwords, freeing up support resources for other issues.  Increased Security: The password recovery feature can be designed to be secure and to prevent unauthorized access to user accounts, reducing the risk of data breaches and other security incidents.  Compliance: Implementing a secure password recovery feature can help the system comply with legal and regulatory requirements related to data protection and privacy.  Competitive Advantage: Providing a password recovery feature can be a competitive advantage, as it demonstrates the system's commitment to user security and user experience. | | | | | |
| Expected Workflow: User navigates to the login page and clicks on the "Forgot Password" link.  The system prompts the user to enter their email address or username associated with their account.  The system verifies the user's identity by sending a secure password recovery link to the email address associated with the user's account or by asking security questions that only the user can answer.  The user receives the secure password recovery link and clicks on it to be redirected to the password reset page.  The system prompts the user to create a new password that meets the password complexity rules defined by the system.  The user enters a new password and confirms it.  The system verifies the new password meets the complexity rules and saves the new password.  The system confirms to the user that their password has been reset successfully.  The user is redirected to the login page and can now use their new password to log in to the system. | | | | | |
| Test Scenarios: Verify that the "Forgot Password" link is visible and functional on the login page.  Verify that the user is prompted to enter their email address or username associated with their account to initiate the password recovery process.  Verify that the system sends a secure password recovery link to the email address associated with the user's account.  Verify that the password recovery link is valid and secure and can only be used once.  Verify that the user can reset their password using the password recovery link.  Verify that the user is prompted to create a new password that meets the password complexity rules defined by the system.  Verify that the user is required to confirm their new password to prevent mistakes.  Verify that the system verifies the new password meets the complexity rules and saves the new password.  Verify that the system confirms to the user that their password has been reset successfully.  Verify that the user can log in to the system using their new password. | | | | | |
| BA: | | Nate | | 2/3/2023 | |
| Tester: | | Michael | | 3/2/2023 | |
| Director | | Brian | | 4/20/2023 | |