TEST CASE DOCUMENT

1. **USER MANAGEMENT SUBSYSTEM**
   1. **SIGN UP**

|  |  |
| --- | --- |
| **#** | TS1 |
| **Title** | Verify "Sign up" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to signup |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 | Verify that a new user can successfully sign up | - | User is on the Sign-Up page with valid credentials | The user receives an email verification link | 1. Navigate to the Sign-Up page 2. Select a role (Title Applicant/PRGI Official) 3. Fill in all required fields with valid data 4. Submit the form | The system displays "Check your email to verify your account" and sends a verification email |
| TC2 | Verify that the system prevents duplicate email or username registration | TC1 | A user account with the same email or username already exists | The system prompts the user to enter a different email or username | 1. Navigate to the Sign-Up page 2. Enter an email or username already registered 3. Submit the form | The system displays "Email/Username already registered. Try a different one." |
| TC3 | Verify validation for incorrect email format | TC1 | User enters an invalid email format | The system prompts the user to enter a valid email | 1. Navigate to the Sign-Up page 2. Enter an invalid email (e.g., "user@com" or "userdomain.com") 3. Submit the form | The system displays "Enter a valid email address (example@domain.com)" |
| TC4 | Verify password strength validation | TC1 | User enters a weak password | The system prompts the user to enter a strong password | 1. Navigate to the Sign-Up page 2. Enter a password without uppercase, number, or special character 3. Submit the form | The system displays "Password must be at least 8 characters, including uppercase, lowercase, number, and special character." |
| TC5 | Verify that passwords must match | TC1 | User enters mismatched passwords in "Password" and "Confirm Password" fields | The system prompts the user to ensure passwords match | 1. Navigate to the Sign-Up page 2. Enter a valid password in the "Password" field 3. Enter a different password in the "Confirm Password" field 4. Submit the form | The system displays "Passwords do not match." |
| TC6 | Verify system behaviour if the user does not verify email within 24 hours | TC1 | The user has received a verification email but does not verify within 24 hours | The system deactivates the incomplete registration | 1. Register with a valid email 2. Do not verify within 24 hours 3. Try logging in | The system displays "Email verification expired. Request a new verification link." |
| TC7 | Verify that partially completed registrations are not stored | TC1 | User fills out some fields but leaves the page before submitting | The system does not store incomplete data | 1. Navigate to the Sign-Up page 2. Fill in some fields 3. Close the page without submitting | The system does not save any user data |

* 1. **LOG IN**

|  |  |
| --- | --- |
| **#** | TS2 |
| **Title** | Verify "Log in" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 | Verify that a registered user can log in with correct credentials | - | User is a registered and verified account holder | User is successfully logged in and redirected to the dashboard | 1. Navigate to the login page 2. Select the appropriate role (Title Applicant/PRGI Official/System Administrator) 3. Enter a valid username/email and password 4. Click the "Login" button | The system grants access and redirects the user to their respective dashboard |
| TC2 | Verify that an unregistered user cannot log in | - | The username/email entered is not associated with any registered account | User is not logged in | 1. Navigate to the login page 2. Select any role 3. Enter a non-existent username/email and a random password 4. Click the "Login" button | The system displays: "Invalid username or password. Please try again." |
| TC3 | Verify that a registered user cannot log in with incorrect credentials | - | User is a registered and verified account holder | User is not logged in | 1. Navigate to the login page 2. Select the appropriate role 3. Enter a valid username/email but an incorrect password 4. Click the "Login" button | The system displays: "Invalid username or password. Please try again." |
| TC4 | Verify that an account is temporarily locked after three consecutive failed login attempts | TC3 | User has entered incorrect login credentials three times in a row | User is temporarily locked out | 1. Attempt to log in with incorrect credentials three times consecutively 2. Observe the system's response on the third failed attempt | The system locks the account temporarily and displays: "Too many failed login attempts. Your account is locked for 5 minutes." |
| TC5 | Verify that a user can reset their password using the "Forgot Password" option | - | User is registered but has forgotten their password | User receives a password reset email | 1. Navigate to the login page 2. Click on "Forgot Password?" 3. Enter a valid registered email 4. Click "Submit" | The system sends an email with a password reset link |
| TC6 | Verify that an unverified user cannot log in | - | User is registered but has not verified their email | User is not logged in | 1. Navigate to the login page 2. Select the appropriate role 3. Enter valid credentials for an unverified account 4. Click "Login" | The system displays: "Email verification required. Check your inbox." |
| TC7 | Verify that a session expires after inactivity | - | User is logged in and inactive for 30 minutes | User is logged out automatically | 1. Log in with valid credentials 2. Stay inactive for 30 minutes 3. Attempt to perform an action on the dashboard | The system logs the user out and redirects to the login page with a message**: "Your session has expired. Please log in again."** |

* 1. **LOG OUT**

|  |  |
| --- | --- |
| **#** | TS3 |
| **Title** | Verify "Log out" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to logout |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 | Verify that a logged-in user can log out successfully | - | User is logged into the system | User session is terminated, and they are redirected to the login/ homepage | 1. Log in to the system 2. Click the "Log Out" button 3. Confirm the logout if prompted | The system logs out the user and redirects them to the login/homepage |
| TC2 | Verify that the session expires after inactivity | - | User is logged in and remains inactive for 30 minutes | User is logged out automatically | 1. Log in to the system 2. Stay inactive for 30 minutes 3. Attempt to perform an action after inactivity | The system logs out the user and redirects them to the login page with a message: "Your session has expired. Please log in again." |
| TC3 | Verify that session data is cleared upon logout | TC1 | User has logged out successfully | No session data should persist after logout | 1. Log in to the system 2. Log out using the "Log Out" button 3. Click the browser’s "Back" button or refresh the page | The system prevents access to previous session data and redirects to the login page |
| TC4 | Verify logout functionality after a system crash | - | User was previously logged in before the crash | User must re-login to access the system | 1. Log in to the system 2. Simulate a system crash (e.g., close the browser or restart the system) 3. Reopen the browser and attempt to access the dashboard | The system prompts the user to log in again |
| TC5 | Verify that logout can be cancelled if a confirmation prompt appears | - | User is logged into the system and a logout confirmation message is displayed | User remains logged in | 1. Click the "Log Out" button 2. When the confirmation message appears, click "Cancel" | The system aborts the logout process, and the session remains active |
| TC6 | Verify that multiple logins from different devices are handled properly on logout | - | User is logged in on multiple devices | The session is only terminated on the device where logout is performed | 1. Log in to the system on Device A 2. Log in to the system on Device B using the same account 3. Log out from Device A | The system logs out the user only on Device A, while Device B remains active |

* 1. **RESET PASSWORD**

|  |  |
| --- | --- |
| **#** | TS4 |
| **Title** | Verify "Reset Password" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to reset their account password |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 | Verify successful password reset with valid credentials | - | User is logged in | Password is updated, and the user can log in with the new password | 1. Navigate to Account Settings 2. Click "Reset Password" 3. Enter the correct current password 4. Enter a valid new password and confirm it 5. Submit the form | The system updates the password and displays a success message: "Your password has been successfully updated." |
| TC2 | Verify error when entering an incorrect current password | - | User is logged in | Password remains unchanged | 1. Navigate to Account Settings 2. Click "Reset Password" 3. Enter an incorrect current password 4. Click Submit | The system displays an error message: "Incorrect current password. Please try again." |
| TC3 | Verify error when new password does not meet security criteria | - | User is logged in | Password remains unchanged | 1. Navigate to Account Settings 2. Click "Reset Password" 3. Enter the correct current password 4. Enter a weak new password (e.g., "password123") 5. Click Submit | The system displays an error message: "Password must be at least 8 characters long and include uppercase, lowercase, a number, and a special character." |
| TC4 | Verify error when new password and confirmation do not match | - | User is logged in | Password remains unchanged | 1. Navigate to Account Settings 2. Click "Reset Password" 3. Enter the correct current password 4. Enter a valid new password 5. Enter a mismatched confirmation password 6. Click Submit | The system displays an error message: "New password and confirmation do not match. Please re-enter both fields." |
| TC5 | Verify that the user can cancel the reset process | - | User is logged in and initiates the password reset | Password remains unchanged | 1. Navigate to Account Settings 2. Click "Reset Password" 3. Click "Cancel" instead of submitting the form | The system aborts the reset process, and no changes are made |
| TC6 | Verify that the user must log in with the new password after a reset | TC1 | User has successfully reset their password | The user must use the new password to log in | 1. Reset the password successfully 2. Log out 3. Try logging in with the old password (should fail) 4. Try logging in with the new password (should succeed) | The system prevents login with the old password and grants access with the new one |
| TC7 | Verify session handling after a successful password reset | TC1 | User is logged in and resets the password | The system may log out the user to re-authenticate with the new password | 1. Navigate to Account Settings 2. Click "Reset Password" 3. Successfully reset the password 4. Check if the system logs out the user automatically | The system either logs out the user or prompts for re-authentication with the new password |

* 1. **MANAGE USER ACCOUNTS**

|  |  |
| --- | --- |
| **#** | TS5 |
| **Title** | Verify "Managing User Accounts" functionality |
| **Description** | To test the different scenarios that might arise while a system administrator is trying to manage the accounts of the system users |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 | Verify that the system administrator can successfully restrict a user account | - | Admin is logged in | User account is restricted, and access is limited | 1. Navigate to User Management 2. Select a user account 3. Click "Restrict Account" 4. Confirm the action | The system restricts the account and displays: "User access has been temporarily restricted." |
| TC2 | Verify that the system administrator can delete a user account permanently | - | Admin is logged in | User account is deleted and no longer exists in the system | 1. Navigate to User Management 2. Select a user account 3. Click "Delete Account" 4. Confirm the action | The system removes the user and displays: "User account successfully deleted." |
| TC3 | Verify that the system administrator can block a user account indefinitely | - | Admin is logged in | User account is blocked, and the user cannot log in | 1. Navigate to User Management 2. Select a user account 3. Click "Block Account" 4. Confirm the action | The system blocks the user and displays: "User account has been blocked indefinitely." |
| TC4 | Verify that the system administrator can verify a PRGI Official’s account | - | Admin is logged in | PRGI Official’s account is verified | 1. Navigate to User Management 2. Select a PRGI Official’s account 3. Click "Verify Account" 4. Review credentials and approve verification | The system verifies the account and displays: "PRGI Official verification successful." |
| TC5 | Verify that the system administrator can grant official access to a Title Applicant | - | Admin is logged in | The applicant’s account is upgraded to an official account | 1. Navigate to User Management 2. Select a Title Applicant’s account 3. Click "Grant Official Access" 4. Confirm the action | The system upgrades the account and displays: "User has been granted official access." |
| TC6 | Verify system response when attempting to manage a non-existent user account | - | Admin is logged in | Error message is displayed, and no action is performed | 1. Navigate to User Management 2. Search for a non-existent user 3. Attempt to manage the account | The system displays: "User account not found. Please search again." |
| TC7 | Verify that the administrator cannot perform unauthorized actions | - | Admin is logged in but lacks permissions for a certain action | No changes are made, and an error message is displayed | 1. Navigate to User Management 2. Attempt an action without proper authorization | The system displays: "You do not have permission to perform this action." |
| TC8 | Verify that an administrator can revert a restriction or unblock an account | TC1/TC3 | User account is restricted or blocked | User account is reactivated | 1. Navigate to User Management 2. Select a restricted/blocked user 3. Click "Unrestrict/Unblock" 4. Confirm the action | The system restores the account and displays: **"User account has been reactivated."** |

* 1. **MANAGE PREFERENCES IN SETTINGS**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 | Verify that a user can successfully update personal information in Account Settings | - | User is logged in | Personal details are updated | 1. Navigate to Settings > Account Settings 2. Update name, email, or contact details 3. Save changes | The system updates details and displays: "Account information updated successfully." |
| TC2 | Verify that a user can change their password successfully | - | User is logged in | Password is changed, and the user must log in with the new password | 1. Navigate to Settings > Account Settings 2. Click Change Password 3. Enter current and new password 4. Confirm and save changes | The system updates the password and displays: "Password changed successfully. Please log in again." |
| TC3 | Verify that a user can enable or disable two-factor authentication (2FA) | - | User is logged in | 2FA is enabled or disabled as per user choice | 1. Navigate to Settings > Account Settings 2. Toggle the Two-Factor Authentication option 3. Confirm selection | The system applies changes and displays: "Two-Factor Authentication updated successfully." |
| TC4 | Verify that a user can manage notification preferences (Email, SMS, In-App) | - | User is logged in | Notification preferences are updated | 1. Navigate to Settings > Notification Preferences 2. Enable/Disable Email, SMS, or In-App notifications 3. Save changes | The system updates preferences and displays: "Notification settings updated successfully." |
| TC5 | Verify that a user can update privacy settings (data visibility and sharing preferences) | - | User is logged in | Privacy settings are updated | 1. Navigate to Settings > Privacy Settings 2. Modify data-sharing and visibility preferences 3. Save changes | The system updates privacy settings and displays: "Privacy settings updated successfully." |
| TC6 | Verify that a user can customize UI themes and accessibility features | - | User is logged in | UI changes are applied | 1. Navigate to Settings > Display & Accessibility 2. Change theme, font size, or enable accessibility features 3. Save changes | The system applies settings and displays: "Display preferences updated successfully." |
| TC7 | Verify that a non-admin user cannot modify system-level configurations | - | Non-admin user is logged in | System settings remain unchanged | 1. Navigate to Settings > System Configurations 2. Attempt to modify system-level settings | The system blocks the action and displays: "You do not have permission to modify system configurations." |
| TC8 | Verify that an invalid email format is not accepted while updating account settings | - | User is logged in | Error message is displayed; changes are not saved | 1. Navigate to Settings > Account Settings 2. Enter an invalid email format (e.g., invalidemail@com) 3. Save changes | The system displays an error: "Invalid email format. Please enter a valid email." |
| TC9 | Verify that a user can cancel changes before saving | - | User is logged in | No changes are applied | 1. Navigate to Settings 2. Modify any preference 3. Click Cancel instead of saving | The system discards changes and displays: **"No changes were applied."** |

1. **TITLE SUBMISSION & VERIFICATION SUBSYSTEM**
   1. **SUBMIT TITLE FOR VERIFICATION**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **VIEW SIMILARITY SCORE**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **VIEW VERIFICATION PROBABILITY**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **RECEIVE FEEDBACK ON REJECTED TITLES**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **VIEW VERIFICATION RESULT**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **MODIFY AND RESUBMIT TITLE**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **REGISTER TITLE**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **TRACK SUBMISSION HISTORY**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. **TITLE COMPLIANCE & MODERATION SUBSYSTEM**
   1. **SEARCH AND VIEW EXISTING TITLES**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **FLAG REJECTED TITLES**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **MANAGE DISALLOWED WORDS**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **MANAGE DISALLOWED AFFIXES**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **SET/MODIFY ACCEPTANCE PROBABILITY**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **REVIEW FLAGGED TITLE SUBMISSIONS**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **OVERRIDE SYSTEM DECISIONS**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. **REPORTING & ANALYTICS SUBSYSTEM**
   1. **VIEW SUBMISSION REPORTS & TRENDS**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **AUDIT USER ACTIVITY & LOGS**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. **SYSTEM ADMINISTRATION & SECURITY SUBSYSTEM**
   1. **CONFIGURE SYSTEM SETTINGS**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **MONITOR & OPTIMIZE DATABASE PERFORMANCE**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **ENSURE SECURITY & COMPLIANCE**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. **SUPPORT & HELP SUBSYSTEM**
   1. **ACCESS HELP & GUIDELINES**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **CONTACT SUPPORT**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

* 1. **MANAGE USER SUPPORT REQUESTS**

|  |  |
| --- | --- |
| **#** | TS |
| **Title** | Verify "" functionality |
| **Description** | To test the different scenarios that might arise while a user is trying to login |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **#** | **Summary** | **Dependency** | **Pre-condition** | **Post-condition** | **Execution Steps** | **Expected Output** |
| TC1 |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |