Functional Testing: End-to-End Scenario-based Testcases

1. **General**
   a. **Color Coding**
      i. The error messages throughout the system should be highlighted in RED
      ii. The success messages throughout the system should be highlighted in GREEN
      iii. Any notices or additional information for the user should be highlighted in YELLOW
      iv. Any menu items and system information should be highlighted in BLUE
      v. Any user inputs and search queries should be highlighted in WHITE

   b. **MOTD / Banner**
      i. The Banner Message is displayed properly
      ii. The TOS and Privacy Policy Links are displayed properly
      iii. Both links lead to their respective (static) documents
      iv. When pressing "n" on the prompt, the program exits
      v. When pressing "y" on the prompt, the login window appears

   c. **Login**
      i. When logging in with an invalid username, prints error "Username is invalid"
      ii. If username valid but not found, prints error "Unknown Username / Password combination"
      iii. If username is found, but incorrect password is entered, prints error "Unknown Username / Password combination"
      iv. If password is entered 3x incorrectly for the same username, locks user and prints error "Maximum amount of attempts has been reached"
      v. LOG creation for account locked event (authlogs)
      vi. If user tries to log into a deactivated account, prints error "User is deactivated"
      vii. LOG creation for login attempt on deactivated account (authlogs)
      viii. If user tries to log into a deactivated account, prints error "User is currently locked"
      ix. LOG creation for login attempt on locked account (authlogs)
      x. If username and password combination is valid, the user should be greeted by his/her first name and redirected to the role-specific main menu view
      xi. LOG creation for successful login (authlogs)
      xii. If user logs in for the first time, prompts user to change password

   d. **Password Change**
      i. User needs to enter current password before proceeding with the new password entry
      ii. New password and confirm password have to be identical, else prints error message "passwords do not match"
      iii. New password and old password must differ, else prints error message "may not be the same as old one"
      iv. New password must confirm to password validation rules, else prints error "does not confirm with the system's password standards"
      v. If password change has been successful, prints confirmation and logs user out of the system

<ol type="i" start="6">
<mark>LOG</mark> creation for successful password change (authlogs)
<mark>EMAIL</mark> notification to user is sent, to inform of successful password change

e. Logout
<ol type="i">
Choosing the menu option "Logout" prints message "Thank you for using the NCSC Suspect Sources System. See you soon, {firstname}!"
Application exits after displaying the notice

2. Administrator Role

a. User Creation
<ol type="i">
Choosing the menu option "Create New User" displays user creation prompt
First and Last Name inputs should only accept names that meet the validation rules: *>2 characters and may only contain letters, spaces and '-'*
Date of birth input should only accept a dob if validation is met: *exactly 10 characters and may only contain numbers and '-'*
Email input must meet: *contain exactly 1x '@' and at least 1x '.' and end with a letter. May contain letters and number, as well as the special characters: '-', '.', '_', '+'*
If any validations are not met, displays error and asks for that specific input again
If user creation was successful, prints message "User has successfully been created!"
<mark>LOG</mark> creation for successful user creation (adminlogs)
<mark>EMAIL</mark> notification to new user is sent, containing username and password
Displays question "Do you want to create another user?"
If "y" is chosen: restarts the user creation process
If "n" is chosen: returns to the administrator main menu

b. User Modification
<ol type="i">
Choosing the menu option "Modify Existing User" displays edit user prompt
Email input appears to select the user to be modified
Entered email has to conform to email validation rules
If no user found for the given email, prints error "No User found for the email address"
If user was found, prints according user information (id, first name, last name, email, dob, current status)
Lists options of user information to be changed
Depending on attribute choice asks for new value input which confirms to the validation rules
If value does not confirm to validation rules, prints error
If option "Cancel" is chosen returns to main administrator menu
If value is valid, prints message "User has successfully been modified!"
<mark>LOG</mark> creation for successful user creation containing attribute and values changed (adminlogs)
Displays question "Do you want to modify another user?"
If "y" is chosen: restarts the user modification process
If "n" is chosen: returns to the administrator main menu

    c. Deactivate User

        i. Choosing the menu option "Deactivate User" displays the user deactivation prompt
        ii. Email input appears to select the user to be deactivated
        iii. Entered email has to conform to email validation rules
        iv. If no user found for the given email, prints error "No User found for the email address"
        v. If user is already deactivated prompt error message
        vi. If user was found and is currently not deactivated, prints according user information (id, first name, last name, email, current status)
        vii. Prompt for confirmation: "Are you sure you want to deactivate this user?"
        viii. If "y", and deactivation was successful, should display success message "User has successfully been deactivated"
        ix. LOG creation for successful user deactivation (adminlogs)
        x. Displays question "Do you want to deactivate another user?"
        xi. If "y" is chosen: restarts the user deactivation process
        xii. If "n" is chosen: returns to the administrator main menu

    d. Unlock User

        i. Choosing the menu option "Unlock User" displays the user unlock prompt
        ii. Email input appears to select the user to be unlocked
        iii. Entered email has to conform to email validation rules
        iv. If no user found for the given email, prints error "No User found for the email address"
        v. If user is currently not unlocked, prompt error message
        vi. If user was found and is currently locked, prints according user information (id, first name, last name, email, current status)
        vii. Prompt for confirmation: "Are you sure you want to unlock this user?"
        viii. If "y", and unlock was successful, should display success message "User has successfully been unlocked"
        ix. LOG creation for successful user unlock (adminlogs)
        x. Displays question "Do you want to unlock another user?"
        xi. If "y" is chosen: restarts the user unlock process
        xii. If "n" is chosen: returns to the administrator main menu

3. Specialist Role

    a. Search Source

        i. Choosing the menu option "Search Source" should display the search prompt
        ii. The prompt should display all attributes the user can search by
        iii. The user then can select his/her attribute of choice and will be prompted to input the value to search for
        iv. Search inputs have to meet validation rules, else print error and ask user to input a valid value again
        v. If source entries are found for search term, lists all ids and names of results
        vi. Prompts user to input specific Id to view source information and details
        vii. If invalid id is given, prints error message "Invalid source id"

viii. If valid id that is part of the results table, prints back source information in detail (including description, url, creation/modification date and threat level)

ix. LOG creation for successfully viewing source entry (operationlogs)

x. Prompts user for editing source information, searching for new source, or returning to main specialist menu

xi. If new search is selected, restart search process

xii. If main menu is selected, return to main specialist menu

xiii. If edit source is selected, display edit source options for this specific source entry

b. **Modify Existing Source**

i. When edit is selected, displays edit prompt for displayed source entry

ii. Displays options to select attribute to be changed

iii. Depending on attribute choice, input follows validation rules

iv. If validation is not met, displays error message

v. If successful, prints message "Source has been modified successfully"

vi. LOG creation for successful source modification (operationlogs)

vii. After modification, sends user back to Main Specialist Menu

c. **Create Source Entry**

i. Choosing the menu option "Create Source" displays the source creation prompt

ii. The creation inputs should follow the validation rules

iii. URL needs to be entered with leading "http:"

iv. If validation rule is not met, prompt error message and ask for correct input

v. If all inputs are correct, displays success message "Source has successfully been created!"

vi. EMAIL notification sends out to all users with role "Authority" notifying of the new source created in the system.

vii. LOG creation for successful source creation (operationlogs)

viii. Displays question "Do you want to create another source?"

ix. If "y" is chosen: restarts the source creation process

x. If "n" is chosen: returns to the specialist main menu

4. **External Authority Role**

a. **Search Source**

i. Choosing the menu option "Search Source" should display the search prompt

ii. The prompt should display all attributes the user can search by

iii. The user then can select his/her attribute of choice and will be prompted to input the value to search for

iv. Search inputs have to meet validation rules, else print error and ask user to input a valid value again

v. If source entries are found for search term, lists all ids and names of results

vi. Prompts user to input specific Id to view source information and details

vii. If invalid id is given, prints error message "Invalid source id"

        viii. If valid id that is part of the results table, prints back source information in detail (including description, url, creation/modification date and threat level)

        ix. <mark>LOG</mark> creation for successfully viewing source entry (operationlogs)

        x. Prompts user for either searching for new source, or returning to main authority menu

        xi. If new search is selected, restart search process

        xii. If main menu is selected, return to main authority menu

        xiii. **!!!** Ensure no source edit option is given

5. **Email Notification Templates**

    a. **Registration Email**

        i. Email Template is in the correct format

        ii. Email includes valid username and password

        iii. Email includes first name in Subject line

        iv. Email includes first name in address line

        v. Email includes correct signature format

    b. **Source Creation Email**

        i. Email Template is in the correct format

        ii. Email includes all source specific information: name, id, url, threat_level

        iii. Email includes source name in Subject line

        iv. Email includes first name of recipient in address line

        v. Email includes correct signature format

    c. **Change Password Confirmation**

        i. Email Template is in the correct format

        ii. Email includes first name in address line

        iii. Email has subject "Password Changed Successfully"

        iv. Email includes correct signature format