***Verify the number of characters for the password matches user specifications***

**Input:** The User inputs a request for a password of a certain length to the password generation system. The system then runs this request as a process and completes or fails to provide a password of the specified length given by the user

**Output:** If the password generation system successfully produces a password based on the user input and the length of the generated password = user specified length, the test succeeds. If the system does not return a password = user specified length or doesn’t return a password at all the test fails (note. The password generation system will not generate a password of a length less than 8 characters and this error will fall under the test case for invalid password length)

***Verify Password functionality for a minimum password length***

**Input:** The Password generation system should have a minimum password length for the customized password as well as the randomized password length. For this system the minimum password length should be 8 characters.

**Output:** If the system can produce a password of a length less than 8 characters this test fails, if the system does not allow for a password length of less than 8 characters, this test is successful (This restriction coincides with the test for invalid password lengths)

***Verify Password functionality for a maximum password length***

**Input:** The Password generation system should have a maximum password length for the customized password as well as the randomized password length. For this system the maximum password length allowed should be 30 characters

**Output:** If the system can produce a password of a length greater than 30 characters this test fails, if the system does not allow for a password length of greater than 30 characters, this test is successful (This restriction coincides with the test for invalid password lengths)

***Test for invalid password lengths***

**Input:** The password generation system should be tested to catch invalid password length requests for the customized password. For this system, the restrictions for password length is that the generated passwords should always be between 8-30 characters and should not go under the minimum or over the maximum. If it does a message should be sent to the user detailing valid password length requests

**Output:** If the password generation system cannot catch invalid password length requests and it causes the system to break, this test fails, if the system does not break from an invalid password length request but does not display the error message to users, this test fails, If the password generation system is able to successfully identify invalid password length requests and also display the error message to prompt users to enter a valid length request, the test is successful

***Check that customized password request requires user specifications***

**Input:** The password generation system for the customized password should require users to select from given fields in order to specify customization for their password(i.e. The system requires users to specifically click on at least one field node in order to produce a customized password)

**Output:** If the system allows for users to generate customized passwords without the user clicking on at least one of the field nodes (i.e. symbols, numbers, uppercase letters, etc.), this test fails. If the system does not allow users to generate customized passwords without specifying fields and displays a message prompting the user to select a field before they can generate a customized password, the test is successful

***Test that customized password allows for inclusion of symbols***

**Input:** The Customized password field nodes should include a node that specifically will include symbols in a requested customized password. A user should be able to select this node and symbols will be included in their custom password as a result.

**Output:** If the system does not successfully allow for the inclusion of symbols into a customized password, the test fails(i.e. The node is selected but symbols aren’t included in the generated password), if the test does allow for the inclusion of symbols in a custom password when the user selects this field node and successfully produces a password with symbols included this test is successful

***Test that customized password allows for inclusion of numbers***

**Input:** The Customized password field nodes should include a node that specifically will include numbers in a requested customized password. A user should be able to select this node and numbers will be included in their custom password as a result.

**Output:** If the system does not successfully allow for the inclusion of numbers into a customized password, the test fails(i.e. The node is selected but numbers aren’t included in the generated password), if the test does allow for the inclusion of numbers in a custom password when the user selects this field node and successfully produces a password with numbers included this test is successful

***Test that customized password allows for inclusion of uppercase letters***

**Input:** The Customized password field nodes should include a node that specifically will include uppercase letters in a requested customized password. A user should be able to select this node and uppercase letters will be included in their custom password as a result.

**Output:** If the system does not successfully allow for the inclusion of uppercase letters into a customized password, the test fails(i.e. The node is selected but uppercase letters aren’t included in the generated password), if the test does allow for the inclusion of uppercase letters in a custom password when the user selects this field node and successfully produces a password with uppercase letters included this test is successful