# Test Plan/Test Approach for nu3 Login Functionality

### 1. Objective:

* Verify the functionality and security of the login feature on the nu3 website <https://www.nu3.de/account/login>

### 2. Scope:

* Focus on the login page at https://www.nu3.de/account/login
* Test across multiple browsers (Chrome, Firefox, Safari) and devices (desktop, mobile)

### 3. Test Environment:

* Operating Systems: Windows, macOS, Android, iOS.
* Browsers: Chrome, Firefox, Safari
* Devices: Desktop, Laptop, Tablet, Mobile

### 4. Functional Tests:

### Positive Test Cases:

* Verify successful login with valid email and password
* Check if the system handles different case variations in the email/username
* Validate login with a combination of alphanumeric characters in the password
* Check Reset password flow for successful re-login

### Negative Test Cases:

* Attempt login with an invalid email
* Attempt login with an incorrect password
* Verify system response when and both email and password is entered blank
* Verify system response to simultaneous multiple login attempts

### 5. Security Tests:

* Ensure the password is not visible in the URL or request parameters
* Test for SQL injection and other common security vulnerabilities

### 6. User Interface/Usability Tests:

* Validate the appearance and responsiveness of the login page on different screen sizes
* Confirm the visibility and usability of the login elements (Email, password, submit etc)
* Check for appropriate error messages on unsuccessful login attempts

### 7. Session Management Tests

* Test the session timeout functionality
* Check if logging out terminates the session correctly

### 8. Additional Testing types can be considered based on Business requirements scope and available project timelines like:

* Compatibility Testing
* Automation Testing
* Performance Testing:
* Compatibility

### 9. Documentation:

* Maintain detailed test documentation, including test cases, results and any bugs found
* Provide clear steps to reproduce any identified issues

### 10. Review and Approval:

* Review the test plan with stakeholders and obtain their approval before execution

### 11. Execution:

* Execute the prepared detailed test cases systematically while recording results and any deviations from expected behavior

### 12. Bug Tracking:

* Use a bug tracking tool to log and monitor any issues discovered during testing

### 13. Regression Testing:

* Perform regression testing after any fixes or updates to ensure the continued integrity of the login functionality

### 14. Exit Criteria:

### All test cases executed successfully

* No critical security vulnerabilities found
* Test artifacts and documentation finalized
* Approved by stakeholders