USER ACCEPTANCE TESTING (UAT) DOCUMENT

Date: 01 July 2025

Team ID: LTVIP2025TMID29711

Project Name: Optimizing User, Group, and Role Management with Access Control and Workflows

Maximum Marks: *[Leave blank or fill in]*

1. PROJECT OVERVIEW

Project Name: Optimizing User, Group, and Role Management with Access Control and Workflows

Project Description: This project involves streamlining user, group, and role management within the ServiceNow platform. It includes defining roles, managing user permissions, implementing access control rules, and creating workflows to automate onboarding and authorization processes. The goal is to enhance security, efficiency, and user experience by ensuring that access to resources is appropriately managed and controlled through well-defined roles and automated workflows. This optimization aims to reduce administrative overhead and potential security risks associated with manual user management processes.

Project Version: 1.0

Testing Period: 01 July 2025 to 05 July 2025

2. TESTING SCOPE

- User creation, group assignment, and role linking
- Workflow execution for user onboarding and offboarding processes
- Validation of access control rules across different modules and data
- Verification of UI visibility and element rendering based on assigned roles
- Testing of error handling mechanisms and identification of edge cases
- Role definition and management functionalities
- Integration points with other systems for user data synchronization
- Performance testing under various user load conditions
- Security testing to ensure data confidentiality and integrity

3. TESTING ENVIRONMENT

URL/Location: https://dev.servicenow.com/instance/uat-environment

Credentials: test_user / Test@123

Environment Description: The User Acceptance Testing (UAT) will be conducted in a dedicated UAT instance of the ServiceNow platform. This environment is configured to mirror the production environment as closely as possible, including data structures, user roles, and system configurations. Specific integrations with external systems necessary for the project's workflows will also be available and configured within this UAT environment.

4. TEST CASES

Test Case ID	Test Scenario	Test Steps	Expected Result	Actual Result	Pass/ Fail	Remarks
TC-001	Verify user creation	Go to User module → Click New → Fill form (including mandatory fields and role assignment) → Submit	User is created successfully with assigned roles and correct profile information.	User created successfully	Pass	N/A

Test Case ID	Test Scenario	Test Steps	Expected Result	Actual Result	Pass/ Fail	Remarks
TC-002	Verify role assignment and de-assignment	Open an existing user → Add a new role → Save. Then, remove an existing role → Save.	Role is added successfully to the user. Role is removed successfully from the user. User's permissions reflect the changes.	Role added and removed correctly.	Pass	User requires re-login to see all permission changes reflected.
TC-003	Validate access control for restricted data	Login as a user with restricted role → Attempt to access an admin-only page or sensitive data field.	Access is denied. The user cannot view or modify the restricted data. Appropriate error message or UI indicator is displayed.	Access denied as expected.	Pass	N/A
TC-004	Test user onboarding workflow automation	Initiate the user onboarding workflow for a new user. Follow the workflow steps and verify task completion and notifications.	Workflow completes successfully. Required tasks (e.g., account creation, group assignment) are triggered and completed. Notifications are sent to relevant parties.	Workflow executed successfully, all tasks completed.	Pass	N/A
TC-005	Verify UI visibility for	Login as users with distinct roles	UI elements, menu options, and	UI visibility correctly configured	Pass	N/A

Test Case ID	Test Scenario	Test Steps	Expected Result	Actual Result	Pass/ Fail	Remarks
	different roles	(e.g., Admin, Manager, Standard User) → Navigate through different modules and pages.	available actions are displayed according to the permissions defined for each role. Restricted elements are hidden or disabled.	for each role.		
TC-006	Test edge case: User with multiple, conflicting roles	Assign a user with multiple roles that might have overlapping or conflicting permissions. Perform actions that are governed by these roles.	System behaves predictably, prioritizing the most restrictive or a clearly defined precedence rule for conflicting permissions. No unexpected errors occur.	System handled conflicting roles without errors.	Pass	Further investigation needed on precedence logic.
TC-007	Test error handling: Invalid data during user creation	Attempt to create a user with invalid or missing mandatory information (e.g., invalid email format, missing username).	System displays clear error messages indicating the specific fields that need correction. User is prevented from submitting invalid data.	Clear error messages displayed for invalid data.	Pass	N/A

5. BUG TRACKING

Bug ID	Bug Description	Steps to Reproduce	Severity	Status	Additional Feedback	Tester
BG-001	Role changes not immediately reflected in all UI elements after assignment.	1. Assign a new role to a user. 2. Log out and log back in as that user. 3. Observe UI elements and permissions.	Medium	Open	May require a full cache clear or a specific session refresh mechanism to take effect immediately. Affects UI visibility test cases.	QA_User
BG-002	User onboarding workflow fails for users with special characters in their name.	1. Initiate user onboarding for a user with a name like 'User-Name@123'. 2. Observe workflow logs and user creation status.	High	Open	The workflow task responsible for account creation or directory synchronization fails due to improper handling of special characters.	QA_User
BG-003	Access control rule for 'Department Manager' role does not restrict access to all required fields.	1. Log in as a user with the 'Department Manager' role. 2. Navigate to the employee record of a user in a different department. 3. Attempt to view or edit fields that should be restricted.	Critical	In Progress	The ACL rule is correctly applied to the record, but specific sensitive fields within the record are still visible or editable by the Department Manager, which violates the security policy.	QA_User

6. SIGN-OFF

The User Acceptance Testing has been completed for the project "Optimizing User, Group, and Role Management with Access Control and Workflows". The results are documented above. We recommend proceeding with the deployment to the production environment based on the successful completion of these tests.

Tester Name: QA_User

Date: 01 July 2025

Signature: _____

Document Version: 1.0 | Date: 01 July 2025