**Validation**

**1. Client Module Validations**

**Login:**

✅ Ensure the username and password are not empty.

✅ Validate that the username exists in the database.

✅ Check if the password matches the stored hashed password.

**Creating a New Service Request:**

✅ Client ID Validation: Format should be Client0001.

✅ Request Titile: Cannot be empty.

✅ Description: Should be at least 20 characters.

✅ Auto-generated Ticket Number: Ensure uniqueness using UUID or incremented values.

**Viewing Request Status:**

✅ Ensure the client ID is valid before fetching request details.

✅ Prevent unauthorized access (clients should only see their own tickets).

**Responding to Vendor Clarifications:**

✅ Ensure responses are not empty.

✅ Allow response updates only if the request is still In Process.

**2. Vendor Module Validations**

**Login:**

✅ Validate username/password as per client login validation.

**Viewing Service Requests:**

✅ Ensure the vendor can only view unassigned or relevant tickets.

✅ Sort tickets by status (Pending, In Process, Resolved).

**Asking for Clarifications:**

✅ Ensure a valid ticket number is provided.

✅ Prevent asking for clarification on Resolved tickets.

**Providing Solutions:**

✅ Ensure a valid ticket number and status check before updating.

✅ Ensure the solution description is meaningful (minimum 30 characters).

**Updating Ticket Status:**

✅ Allow transitions only in a valid order:

Pending → In Process

In Process → Resolved

**3. General System Validations**

✅ Prevent SQL Injection by using Prepared Statements in JDBC.

✅ Enforce Strong Passwords (Minimum 8 characters, mix of letters, numbers, symbols).

✅ Session Management to prevent unauthorized access.

✅ Ensure Database Constraints (e.g., unique ticket numbers, valid foreign keys).