**🧩 DATABASE: UserManagement**

**🗃️ Tables Needed**

**1. Users**

* Stores user accounts.
* Fields: User info, email, hashed password, role, lock status, login attempts, first login flag, timestamps.

**2. Roles**

* Stores predefined roles (Admin, HR, Manager, Chief Cleaner, Sales Manager).

**3. OTP**

* Stores generated OTPs for two-factor authentication.
* Includes expiry and usage status.

**4. AuditTrail**

* Logs every user and admin action: what was done, by who, when, and from where.

**5. PasswordHistory (optional but highly recommended)**

* Stores past passwords to prevent reuse.
* Helps enforce secure password practices.

**⚙️ Stored Procedures Needed**

**🔧 User Management**

1. sp\_CreateUser – Admin creates user with system-generated password.
2. sp\_AssignRole – Assigns role to user (can be handled in sp\_CreateUser too).
3. sp\_GetUserByEmail – Fetches user by email for login or password reset.

**🔒 Authentication & Security**

1. sp\_AuthenticateUser – Validates email and password; checks lock status.
2. sp\_UpdatePassword – Lets user change password on first login.
3. sp\_RecordFailedLoginAttempt – Increments attempt count, locks after 3 tries.
4. sp\_ResetFailedAttempts – Resets counter after successful login.
5. sp\_UnlockUser – Admin manually unlocks locked accounts.
6. sp\_CheckFirstLogin – Checks if it’s the user’s first login.
7. sp\_CheckPasswordReuse – Prevents reusing old passwords.
8. sp\_AddPasswordHistory – Records each password change.

**🔁 OTP Handling**

1. sp\_GenerateOtp – Generates and stores 6-digit OTP.
2. sp\_ValidateOtp – Verifies OTP correctness and expiry.
3. sp\_InvalidateOtp – Marks OTP as used after verification.

**📋 Audit Logging**

1. sp\_LogAudit – Logs all user and admin actions (login, changes, etc.).

**📂 Role Management**

1. sp\_GetRoles – Lists all available roles for dropdowns or assignment.