DOIT.C
Department of Information Technology & Communication, Rajasthan

GOVERNMENT OF RAJASTHAN
Department of Information Technology & Communication

Rajasthan Single Sign On

Citizen / Pensioner SSO ID Updation Form

(Please read the instructions in given at Page No. 2 of this application form. For SSO ID profile correction Please fill the form in BLOCK/ CAPITAL LETTERS only. Both the pages duly signed by the applicant, should be sent through **Registered Email ID** at **relevant district SSO helpdesk support.)**

Category of the Person (✓ Tick One)	Pensioner/ Citizen
Name of the Applicant	
Address (as per Aadhar card)	
Aadhar card No.	
Janaadhar card No.	
Mobile No.	
Email ID	
Citizen SSOID	
Other (Citizen) SSOID, If any	
Corrections requested in SSO ID:	
Reason for correction in SSO ID	

Only for Pensioners:
Date of Retirement: _______________________________________
Employee ID _________________________________
Pension (PPO) Number: ___________________________________
Government SSO ID (if any): ________________________________

Note: Please attach the following documents along with the application form and send the email to the respective district SSO helpdesk support from user's **registered email ID.**

1. PPO Copy (for pensioner) 2. Aadhar Card 3. Janaadhar Card

Signature of Applicant

Terms and Conditions/Instructions

1. SSOID/ UserID and Password should be kept secret and should not be shared with others even if request on phone or email.
2. A person shall possess only one Single Sign-On (SSO) ID. In case of multiple SSO IDs, the user must merge them to maintain a single active ID.
3. It is recommended, password should be changed at least once in 90 days for SSO. Failure to do so will result in automatic expiration of password and the end-user would not be able to login to his/ her SSO. Also, do not share your username/ password with anyone or in response to any mail that asks for it.
4. Length and Complexity: Passwords must be at least 8 characters long (max. 30 characters) and include a mix of uppercase letters + lowercase letters + digits + special characters.
5. Password must meet the following policies:
    - Lowercase letter (a-z)
    - Uppercase letter(A-Z)
    - Digit (0-9)
    - Special character (~!@#$^=_-)
    - Length 8-30 char
    - Should not be a derivative of easily guessable word or phrase (i.e. 111, 123, aaa, abc, zyx, acca, ACPCA, sso, user, pass, admin, qwerty, test, raj).
    - Should not be a derivative of SSOID, Mobile Number, DOB & EmployeeID (SIPF).
6. Failed Attempts: Accounts will be locked after five failed consecutive login attempts. The default lockout duration will be 30 minutes unless reset by the RajSSO Helpdesk Team. Users will be notified if their account is locked due to failed login attempts.
7. Self-Service: Users can change/reset their passwords on their own after due verification of information provided by them during registration.
8. **Once an SSO ID is deactivated or disabled, it cannot be reactivated.**
9. A Mobile Number, Email ID, JanAadhar ID, or UID cannot be linked to more than one SSO ID.
10. It is suggested for all users to keep their registered Email ID updated in their SSO ID profile.
11. All communications related to applications must be sent exclusively from the Email ID registered with the SSO ID.
12. In case the registered Email ID is not available or updated in the SSO profile, the user must personally visit the nearest District DOIT&C Office (Collectorate) with valid identification proof to update the details.
13. End-users of the SSOID shall be solely responsible for all activities/transactions performed using their SSOID. No users shall permit others to perform any activity/transaction using their SSOID or perform any activity/transaction with SSOID belonging to other users.

Signature of Applicant

Date:______________