RajSSO: Password Policy (w.e.f. 01/06/2024)

1. Purpose

The purpose of this policy is to establish a standard for the creation, management, and use of SSOID passwords on the RajSSO platform and to protect against incidents of Identity Theft arising due to weak SSOID passwords defined by end-users. This policy aims to ensure that SSOID passwords are strong & regularly changed/updated by end-users.

2. Scope

The Scope of this policy includes all the SSOIDs created on the RajSSO Platform.

3. Policy

3.1. Password Creation

3.1.1 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.

3.1.2 Prohibited Passwords: End-users of SSOID to avoid common words, phrases, or easily guessable information such as mobile number, city of birth, DOB, common names etc.

3.1.3 The password shall not be a derivative of the SSOID.

3.1.4 The password shall not be a slang, dialect, jargon etc.

3.1.5 The password shall not be a common usage word such as names of family, pets, friends, co-workers, fantasy characters, etc

3.1.6 The password shall not be based on computer terms and names, commands, sites, companies, hardware, or software.

3.1.7 The password shall not be based on birthdays and other personal information such as addresses and phone numbers.

3.1.8 The password shall not be a word or number pattern like aaabbb, qwerty, zyxwvuts, 123321, etc., or any of the above spelled backward.

3.1.9 Uniqueness: Passwords must be unique and not used for any other accounts, especially external services or websites.

3.2. Password Protection

3.2.1 Confidentiality: Passwords must be kept confidential and should not be shared with any other person/end-user.

3.2.2 Passwords must not be communicated through email messages or other forms of electronic communication.

3.2.3 Storage: Passwords should not be written down or stored in an easily accessible place.

3.2.4 Visibility: Ensure passwords are not visible on screens or shared over unsecured communication channels.

3.2.5 The "Remember Password" feature of web browsers and other applications, wherever available, should not be used.

3.2.6 If the password is shared with support personnel for resolving problems relating to any service, it should be changed immediately after the support session.

3.2.7 The password should be changed immediately if it is suspected of being disclosed, or known to have been disclosed to an unauthorized user.

3.3. Password Change

3.3.1 Regular Updates: Passwords must be forcibly changed at least every 90 days.

3.3.2 Event-Driven Changes: Change passwords immediately if there is any suspicion that they may have been compromised.

3.3.3 Unique Changes: When changing passwords, the new password must be significantly different from the previous passwords. A minimum of the last five passwords cannot be reused.

3.3.4 Notifications: Users will be notified for each password change/reset event.

3.4. Account Lockout

3.4.1 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.

3.4.2 Notification: Users will be notified if their account is locked due to failed login attempts.

3.5. Multi-Factor Authentication (MFA)

3.5.1 Requirement: It is highly recommended that Multi-Factor Authentication (MFA) be enabled by end-users for authentication on the RajSSO Portal. This provides an additional layer of security to the end-user.

3.6. Password Recovery

3.6.1 Self-Service: Users can change/reset their passwords on their own after due verification of information provided by them during registration.

4. Other IT Systems and Applications

4.1 All the provisions mentioned in Section-3 of this policy document will also apply to other IT systems/ applications.

4.2 No password shall be traveling in clear text; the hashed form of the password should be used. To get around the possibility of a replay of the hashed password, it shall be used along with a randomization parameter.

4.3 The backend system/database shall store only the hash of the individual passwords and never the plain passwords in readable form.

5. Policy Review

5.1 This policy will be reviewed half-yearly and updated as needed to ensure compliance with security best practices and evolving threats.

6. Responsibilities

6.1 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.