Protean eGov Technologies Limited

Password Policy

for

Central Recordkeeping Agency

Version 1.0

DOCUMENT CONTROL SHEET

Document Name: Password Policy

Sr. No.	Date of Revision	Ver	Section Number	Description of Change
1	Sept, 2024	1.0	-	Initial Version

Table of Contents

1. Overview:-

Protean eGov Technologies Limited (formerly NSDL e-Governance Infrastructure Limited) is committed to ensuring the security of its systems and data. This Password Policy outlines the formal management process for adherence to password security guidelines.

2. Purpose and Objectives:-

Password Policy is to establish a standard for creating, maintaining, and protecting passwords for accessing the systems and data. This policy is designed to enhance security by ensuring that all CRA users follow best practices for password creation and management. The objective of this Password Policy is to protect the integrity, confidentiality, and availability of the information and systems managed by Protean CRA

Password is the first line of access control for any information system. The purpose of this policy is to implement effective password management system. Wherever possible an interactive system shall be established to ensure quality passwords.

3. Scope of the policy: -

This policy is directed towards following Users of CRA system

- Subscriber
- Nodal Offices (Corporate and Government)
- Financial Controller
- Point of Presence – Service Providers (POP-SPs)
- Aggregators
- Atal Pension Yojana - Service Providers (APY-SPs)
- Annuity Service Providers (ASP)
- NPS Trust
- PFRDA

It is applicable for following logins:

- CRA

- NPSCAN
- NPS Lite - APY
- Mobile App

4. Policy Rules:-

4.1 Rules for Passwords: -

Following password rules shall be enforced in Protean-CRA:

- Minimum password length shall be 8 to 16 characters
- At least one upper case (A-Z)
- At least one lower case (a-z)
- At least one number (0-9)
- At least one special characters (!@#$^&*~)
- No space character
- Maximum password age shall be 60 days
- Passwords maintained in databases is stored in hashed form.
- After five consecutive failed login attempts, user account shall be locked out.
- User should be forced to change password on first login
- Maintain a history of last 3 passwords to ensure the users do not repetitively use the old passwords.

4.2 Password Reset:-

Only the individual to whom the User-ID is assigned shall request for User password reset.

4.3 Secure log-on procedures:-

- Log unsuccessful and successful attempts
- Below mentioned message will be shown for Unsuccessful attempts
    - The User Id/I-PIN you have entered is invalid, please try again. For your safety, access to CRA will be locked after 5 consecutive wrong attempts.
- Warning will be shown to the users when one attempt is left
    - One more Password attempt is left
- After account is locked , after 5 consecutive wrong attempts, below mentioned message will be shown

- Your account is locked. To reset the I-PIN, please click on the link 'FORGOT PASSWORD'.

- System will not display a password being entered
- System will not transmit passwords in clear text over a network

4.4 Awareness Programs:

Protean-CRA shall arrange regular training programs to understand the importance of password security. Users shall be educated on the requirements of the password security and the implications of non-compliance.

5. User Responsibilities:-

Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment

5.1 Password Use:-

Users should follow good security practices in the selection and use of passwords. Following guidelines may be used:

- User passwords should remain confidential. Users are responsible for the confidentiality of their passwords. The passwords should not be divulged under any circumstances.
- User should not write password on the desk, near monitor, CPU, under keypad/ keyboard or on a paper and keep it in the drawer.
- Passwords should be changed whenever there is an indication of possible system or password compromise.
- User should not share his/her password with any person. If there is a need to share the password this shall be done after appropriate approvals only.
- Password shall be changed at the earliest on the next working day if password has been shared after appropriate approval to carry out the work in the original user's absence.
- User shall not communicate the password to anybody through e-mail or SMS.

5.2 Password Composition:

- Users should define complex passwords.
- Passwords should be such that they can be easily memorised and typed in without having to look at the keyboard.
- Password should not be based on the following:
  - Family members name.
  - User id.
  - Date of birth.
  - Passport number.
  - Employee code, designation.
  - Department name.
  - Address/ Telephone number.
  - Company name, computer name
  - Full name
  - Pet names
  - Name of favorite animals, colors, flowers, fruits, vegetables, movie stars, etc.
  - Vehicle number
- Password should not be the same as the user's name and ID.
- Password should not be equal to any user's name on the system.

5.3 Unattended User Equipment:

Users should ensure that unattended equipment has appropriate protection. All users should be made aware of the security requirements and procedures for protecting unattended equipment, as well as their responsibilities for implementing such protection.

Following guidelines may be used:

- Users should terminate active sessions before leaving the terminal.
- Screen saver password or similar appropriate locking mechanism should be used to protect unattended equipment
- Users should adhere to Policy on Clear Desk and Clear Screen.

****