Aldan Investments Pvt Ltd
701 Heritage Plaza, Opp. Indian Oil Nagar, JP Road
Andheri (W), Mumbai 400053
CIN: U67120MH1995PTC084811

Password Policy

Version 1.0

1. **Purpose**
   The purpose of this password policy is to establish guidelines and best practices for creating strong passwords and maintaining their security. Passwords play a crucial role in protecting our systems, data, and sensitive information from unauthorized access.

2. **Scope**
   This policy applies to all employees, contractors, and third-party users who have access to [Organization Name]'s systems, networks, applications, and data.

3. **Password Creation**
   3.1 Password Complexity
   - Passwords must be at least 8 characters long.
   - Passwords should include a combination of uppercase and lowercase letters, numbers, and special characters.
   - Avoid using predictable patterns or common words.

   3.2 Password Confidentiality
   - Passwords are confidential and should not be shared with anyone, including colleagues, friends, or family members.
   - Do not write down passwords or store them in easily accessible locations.

   3.3 Unique Passwords
   - Each user must have a unique password for their account.
   - Do not reuse passwords across multiple accounts or systems.

4. **Password Management**
   4.1 Regular Password Changes
   - Users must change their passwords at least every 90 days.
   - Users should not reuse the previous passwords.

   4.2 Password Complexity Refresh
   - Periodically, users will be prompted to update their passwords to meet the current password complexity requirements.
   - This will help ensure passwords remain strong and resistant to unauthorized access.

4.3 Password Reset

- In the event of a forgotten or compromised password, users should follow the organization's password reset procedures.
- Password reset mechanisms should be secure and may involve multifactor authentication or verification of user identity through predetermined methods.

4.4 Prohibited Actions

- Users should refrain from using the following practices:
- Sharing passwords with others.
- Storing passwords in plain text or unsecured files.
- Using easily guessable information such as names, birthdates, or sequential patterns.
- Writing down passwords in unsecured locations.
- Storing passwords in web browsers or other insecure password managers.

5. System Enforcement and Monitoring

5.1 Account Lockouts

- After a certain number of failed login attempts, the user's account will be temporarily locked to protect against brute-force attacks.
- Users must contact the IT support team to have their accounts unlocked.

5.2 Password Expiration Notifications

- Users will receive automated notifications as their password expiration date approaches.
- These notifications will prompt users to change their passwords within the required timeframe.

6. Training and Awareness

Regular training and awareness programs will be conducted to educate users on password security best practices, the importance of strong passwords, and the risks associated with weak passwords.

7. Compliance and Consequences

Failure to comply with this password policy may result in disciplinary action, including temporary or permanent suspension of user accounts and other appropriate measures.