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

User Management Policy

Version 1.0

1. **Purpose:**
- Ensure the secure and efficient management of user accounts and access privileges to IT systems and resources.
- Protect the confidentiality, integrity, and availability of organizational information assets.
- Promote adherence to security policies and best practices.

2. **User Account Provisioning:**
- User accounts will be created based on defined criteria and business needs.
- Access privileges will be assigned according to the principle of least privilege.
- Requests for user account creation will follow an approval process.

3. **User Authentication:**
- Strong authentication mechanisms, such as complex passwords or multi-factor authentication, will be implemented.
- Passwords will be securely stored and transmitted.
- Regular password changes and periodic authentication reviews will be conducted.

4. **User Access Management:**
- Regular reviews of user access rights will be conducted to ensure appropriateness and alignment with job responsibilities.
- User access will be terminated promptly upon employee termination or change in job roles.
- Temporary access privileges will be granted for specific business needs and revoked when no longer required.

5. **Privileged User Management:**
- Privileged access will be tightly controlled and limited to authorized personnel.
- Privileged user activities will be logged and monitored.
- Regular reviews of privileged access rights will be conducted.

6. **User Training and Awareness:**
- Users will receive training on security awareness and the responsible use of IT resources.
- Users will be educated on the importance of protecting their credentials and reporting suspicious activities.
- Regular reminders and updates on security practices will be provided.

7. **Incident Response and User Account Lockouts:**
- Procedures will be in place to respond to and address user account compromises or unauthorized access attempts.
- User accounts may be temporarily locked after a certain number of failed login attempts to prevent brute-force attacks.
- Timely investigation and appropriate action will be taken in response to security incidents involving user accounts.

8. **User Data Privacy:**
- User privacy rights will be respected and protected in accordance with applicable privacy laws and regulations.
- User data will be collected, stored, and processed securely and with consent when required.
- User data will be shared only as necessary and with proper authorization.

9. **User Acceptable Use:**
- Users will be required to adhere to an acceptable use policy that outlines permitted and prohibited activities.
- Monitoring and auditing mechanisms may be implemented to ensure compliance.
- Violations of the acceptable use policy may result in disciplinary actions.

10. **User Account Deactivation and Termination:**
- Processes will be in place to deactivate or delete user accounts promptly upon employee termination.
- Account deactivation will include revoking access privileges and removing user credentials from systems.
- Former employee accounts will be retained for a defined period for auditing and security purposes.