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

Information Security Policy

Version 1.0

1. Purpose:
- Protecting the confidentiality, integrity, and availability of M/s Aldan Investments Private Limited's information assets.
- Ensuring compliance with relevant laws, regulations, and industry standards.
- Mitigating information security risks and safeguarding against unauthorized access, use, disclosure, alteration, or destruction.

2. Scope:
- Applies to all employees, contractors, vendors, and any individual accessing or handling M/s Aldan Investments Private Limited's information assets.
- Covers all forms of information, including electronic, physical, and verbal.

3. Information Classification:
- Classify information into categories based on its sensitivity and criticality.
- Clearly define handling and protection requirements for each category.
- Access controls and security measures will be implemented accordingly.

4. Access Control:
- Implement access controls to ensure authorized access to information.
- Unique user accounts and strong passwords will be used.
- Regular access reviews and account terminations for departed employees will be conducted.

5. Data Protection:
- Encrypt sensitive and confidential data in transit and at rest.
- Regularly back up data and verify the integrity of backups.
- Maintain appropriate data retention and disposal processes.

6. Security Awareness:
- Provide regular information security awareness training to all personnel.
- Promote a culture of security-conscious behavior and adherence to policies and procedures.
- Reporting of security incidents and concerns will be encouraged.

7. Incident Response:
- Establish an incident response plan to address and manage information security incidents promptly.
- Clearly define roles, responsibilities, and escalation procedures.
- Document and learn from security incidents to improve prevention and response.

8. Network and System Security:
- Implement firewalls, intrusion detection systems, and other security controls to protect network and system infrastructure.
- Regularly update and patch systems and applications.
- Conduct vulnerability assessments and penetration testing to identify and remediate vulnerabilities.

9. Physical Security:
- Implement physical access controls to protect premises, data centers, and critical infrastructure.
- Deploy surveillance systems, alarms, and security personnel as appropriate.
- Safeguard against theft, unauthorized access, and environmental hazards.

10. Third-Party Security:
- Assess and monitor the security practices of third-party vendors and service providers.
- Implement appropriate contracts and controls to protect shared information assets.
- Regularly review and update security requirements for third-party engagements.

11. Compliance:
- Comply with applicable laws, regulations, and contractual obligations related to information security.
- Conduct regular audits and assessments to ensure compliance.
- Take necessary steps to address non-compliance and implement corrective actions.