Aldan Investments Pvt Ltd

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

Anti-Virus Policy

Version 1.0

1. **Purpose:**

- Ensure the confidentiality, integrity, and availability of organizational resources and information.
- Establish guidelines for the management and control of user access to systems, networks, and data.
- Minimize the risk of unauthorized access, data breaches, and misuse of resources.

2. **User Access Management:**

- Implement a user access management process that includes user provisioning, modification, and deprovisioning.
- Define roles and responsibilities for granting and revoking access privileges.
- Utilize a centralized user directory or identity management system for efficient access control.

3. **User Authentication:**

- Require strong and unique user authentication for accessing organizational systems and applications.
- Implement multi-factor authentication (MFA) to enhance security.
- Enforce password complexity requirements and regular password changes.

4. **User Access Rights:**

- Assign access rights and permissions based on the principle of least privilege.
- Grant users the minimum level of access required to perform their job functions.
- Regularly review and update access rights to ensure they align with user roles and responsibilities.

5. **Access Control Mechanisms:**

- Implement technical controls to enforce access control policies, such as access control lists (ACLs), firewalls, and intrusion detection systems (IDS).
- Utilize access control technologies, such as role-based access control (RBAC) or attribute-based access control (ABAC), to streamline access management.
- Regularly test and validate the effectiveness of access control mechanisms.

6. Remote Access:

- Establish guidelines and security controls for remote access to organizational systems.
- Utilize secure remote access technologies, such as virtual private networks (VPNs) or secure remote desktop protocols.
- Enforce strong authentication and encryption for remote access connections.

7. Access Monitoring and Logging:

- Implement logging and monitoring mechanisms to record user access activities.
- Regularly review access logs for suspicious or unauthorized activities.
- Define retention periods for access logs based on legal, regulatory, and business requirements.

8. Incident Response and Reporting:

- Establish procedures for reporting and responding to security incidents related to access control.
- Define roles and responsibilities for handling access-related incidents and conducting investigations.
- Promptly report and document security incidents, including unauthorized access attempts or data breaches.

9. Access Control Reviews:

- Conduct periodic access control reviews to ensure the ongoing effectiveness of access control measures.
- Regularly review user access rights, permissions, and privileges.
- Perform user access audits to identify and address any access control violations or discrepancies.

10. Policy Review and Compliance:

- Regularly review the Access Control Policy to ensure it remains aligned with industry best practices, emerging threats, and regulatory requirements.
- Conduct periodic audits to assess compliance with the policy.
- Update the policy as necessary to address changes in technology, business processes, or security threats.