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

Remote Access Policy

Version 1.0

1. **Purpose:**
- Enable secure and authorized remote access to organizational resources, systems, and data.
- Establish guidelines for the use of remote access technologies to maintain productivity and flexibility.
- Ensure the protection of sensitive information and maintain the integrity of organizational systems.

2. **Authorization and Access Control:**
- Remote access must be authorized by the appropriate management or IT personnel.
- Implement strong user authentication mechanisms, such as multi-factor authentication (MFA), for remote access.
- Grant remote access privileges based on job roles and responsibilities, following the principle of least privilege.

3. **Secure Remote Access Methods:**
- Utilize secure remote access technologies, such as virtual private networks (VPNs) or secure remote desktop protocols.
- Implement encryption protocols, such as SSL/TLS, to protect data transmitted over remote access connections.
- Ensure that remote access solutions are regularly updated with the latest security patches and configurations.

4. **User Responsibilities:**
- Remote users must adhere to the organization's acceptable use policy and security guidelines.
- Protect access credentials and use strong passwords for remote access accounts.
- Promptly report any suspected or actual unauthorized access or security incidents.

5. **Endpoint Security:**
- Require remote users to have up-to-date antivirus software and firewall protection on their devices.
- Implement security controls, such as remote device management, to ensure compliance with security policies.
- Educate remote users about the risks of connecting to unsecured networks and provide guidance on secure connectivity.

6. **Data Protection:**
- Encrypt sensitive data transmitted over remote access connections to protect confidentiality.
- Prohibit the storage of sensitive data on remote devices unless authorized and encrypted.
- Implement data loss prevention (DLP) measures to prevent unauthorized data leakage.

7. **Termination of Remote Access:**
- Immediately revoke remote access privileges upon termination or change in employment status.
- Conduct a thorough review and deprovisioning process to ensure removal of all remote access accounts and credentials.
- Implement procedures to collect organizational assets, such as laptops or mobile devices, upon termination or resignation.

8. **Incident Reporting and Response:**
- Establish procedures for reporting and responding to remote access-related security incidents.
- Define roles and responsibilities for handling incidents, conducting investigations, and implementing corrective actions.
- Promptly report and document security incidents related to remote access for further analysis and remediation.

9. **Policy Review and Compliance:**
- Regularly review the Remote Access 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.