Aldan Investments Pvt Ltd

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

Network Security Policy

Version 1.0

1. **Purpose:**

- Protect the confidentiality, integrity, and availability of the organization's network infrastructure and data.
- Establish guidelines for the secure configuration, management, and monitoring of network devices.
- Minimize the risk of unauthorized access, data breaches, and network disruptions.

2. **Network Access Control:**

- Implement access controls, such as firewalls, to restrict unauthorized access to the organization's network.
- Configure network devices to enforce the principle of least privilege for user access.
- Regularly review and update access control lists (ACLs) to reflect the organization's changing requirements.

3. **Network Device Configuration:**

- Follow secure configuration guidelines provided by device manufacturers and industry best practices.
- Change default passwords and disable unnecessary services or protocols on network devices.
- Regularly patch and update network device firmware to address security vulnerabilities.

4. **Wireless Network Security:**

- Implement strong encryption protocols, such as WPA2 or WPA3, for wireless networks.
- Use strong and unique passwords for wireless network access points.
- Regularly review and update wireless network configurations to ensure security controls are effective.

5. **Network Segmentation:**

- Segment the network into secure zones to isolate critical systems and sensitive data.
- Implement network segmentation controls, such as virtual LANs (VLANs) or network segmentation gateways.
- Limit inter-zone communication and establish strict access controls between network segments.

6. Network Monitoring and Logging:

- Implement network monitoring tools to detect and respond to network security incidents.
- Enable logging on network devices to capture relevant security events.
- Regularly review network logs for suspicious activities and incidents.

7. Intrusion Detection and Prevention:

- Deploy intrusion detection and prevention systems (IDPS) to monitor and prevent network attacks.
- Regularly update IDPS signatures and configurations to detect new and emerging threats.
- Establish incident response procedures for handling detected network intrusions.

8. Network Vulnerability Management:

- Conduct regular network vulnerability assessments and penetration tests.
- Patch network devices promptly which address known vulnerabilities.
- Implement a process to track and remediate identified vulnerabilities in a timely manner.

9. Network Backup and Disaster Recovery:

- Implement regular backups of network device configurations and critical network data.
- Store backups securely and test the restoration process periodically.
- Develop and maintain a network disaster recovery plan to ensure network resilience.

10. Employee Awareness and Training:

- Provide network security awareness training to employees to educate them about network security risks and best practices.
- Promote the importance of strong passwords, secure wireless network usage, and safe network browsing habits.
- Encourage employees to report any network security incidents or suspicious activities.

11. Policy Review and Compliance:

- Regularly review the Network Security 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.