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 protection of organizational systems and networks from malicious software threats.
- Establish guidelines for the implementation, configuration, and management of anti-virus solutions.
- Minimize the risk of malware infections and unauthorized access to sensitive information.

2. **Anti-Virus Solution Selection:**

- Evaluate and select an industry-standard, reputable anti-virus solution that meets the organization's needs.
- Consider factors such as effectiveness, compatibility, ease of management, and support capabilities.
- Ensure the chosen solution provides timely updates and comprehensive threat detection capabilities.

3. **Anti-Virus Deployment:**

- Deploy anti-virus software across all organizational systems, including servers, workstations, and mobile devices.
- Utilize centralized management tools to facilitate consistent and efficient deployment.
- Ensure anti-virus software is installed on all new systems during the provisioning process.

4. **Real-Time Protection:**

- Enable real-time scanning and protection to detect and block malware as it enters the system.
- Configure anti-virus software to automatically scan files, emails, and web content in real-time.
- Regularly update anti-virus signatures and scanning engines to ensure optimal threat detection.

5. **Regular Scanning and System Updates:**

- Schedule regular system scans to detect and remove any existing malware infections.
- Configure scans to run during non-business hours to minimize disruptions.
- Apply security patches and system updates promptly to address vulnerabilities that can be exploited by malware.

6. **Quarantine and Remediation:**

- Configure anti-virus software to quarantine infected files or isolate infected systems from the network.
- Establish procedures for the remediation of infected systems, including malware removal and system restoration.
- Provide clear instructions to users on how to report suspected malware incidents.

7. **Security Awareness and Training:**

- Educate employees about the importance of anti-virus protection and the risks associated with malware.
- Provide training on recognizing and reporting suspicious emails, attachments, or websites.
- Encourage employees to promptly report any potential malware incidents or security breaches.

8. **Reporting and Incident Response:**

- Establish procedures for reporting and responding to malware incidents.
- Define roles and responsibilities for handling reported incidents and conducting investigations.
- Maintain records of malware incidents, responses, and remediation actions for future reference.

9. **Software and Signature Updates:**

- Enable automatic updates for anti-virus software and virus signatures.
- Regularly test the updating process to ensure it is functioning correctly.
- Establish monitoring mechanisms to verify that updates are being applied successfully.

10. **Policy Review and Compliance:**

- Regularly review the Anti-Virus 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.

1.