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

# Application Software Policy

## Version 1.0

1. **Purpose:**
- Establish guidelines for the creation, management, and protection of audit trails.
- Ensure the integrity, availability, and confidentiality of audit trail data.
- Support compliance with regulatory requirements and internal control standards.

2. **Audit Trail Generation:**
- Implement mechanisms to capture and record relevant system and user activities.
- Determine the scope of audit trail generation based on regulatory requirements and business needs.
- Define the specific events and actions that will be captured in the audit trail.

3. **Audit Trail Data:**
- Ensure that audit trail data is accurate, complete, and tamper evident.
- Include relevant information such as date, time, user identification, system location, and action details in the audit trail.
- Store audit trail data in a secure and centralized location to prevent unauthorized access or modification.

4. **Retention and Storage:**
- Define retention periods for audit trail data based on legal, regulatory, and business requirements.
- Implement secure storage mechanisms to protect audit trail data from unauthorized alteration or deletion.
- Regularly back up audit trail data and ensure its recoverability in the event of a system failure or data loss.

5. **Access Controls:**
- Implement access controls to restrict access to audit trail data to authorized personnel only.
- Assign responsibilities for managing and monitoring access to audit trail data.
- Maintain logs of individuals who access, modify, or review audit trail data.

6. **Audit Trail Review and Analysis:**
- Establish procedures for regular review and analysis of audit trail data.
- Conduct audits or reviews to identify anomalies, suspicious activities, or non-compliance.
- Utilize automated tools or systems to assist in the analysis of audit trail data.

7. **Monitoring and Alerts:**
- Implement monitoring mechanisms to detect and alert on unusual or suspicious activities captured in the audit trail.
- Configure alerts or notifications for critical events or deviations from established norms.
- Investigate and address potential security breaches or policy violations based on audit trail alerts.

8. **Integration with Incident Response:**
- Integrate audit trail data with incident response processes to support investigations and forensic analysis.
- Define procedures for accessing and preserving audit trail data during incident response activities.
- Ensure audit trail data is admissible as evidence in legal or regulatory proceedings, if required.

9. **Audit Trail Policy Review:**
- Regularly review and update the audit trail policy to align with changing business requirements, technologies, and regulatory landscape.
- Engage relevant stakeholders, including IT, legal, and compliance teams, in the policy review process.
- Conduct periodic audits or assessments to evaluate compliance with the audit trail policy and identify areas for improvement.