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

VAPT & Hardening Policy

Version 1.0

1. **Purpose:**
- Identify vulnerabilities and security weaknesses in the organization's systems, networks, and applications.
- Mitigate risks and strengthen the security posture through regular vulnerability assessment and penetration testing (VAPT) activities.
- Establish guidelines for implementing effective security hardening measures.

2. **VAPT Process:**
- Conduct regular vulnerability assessments to identify potential security weaknesses and vulnerabilities.
- Perform penetration testing to simulate real-world attacks and evaluate the effectiveness of security controls.
- Utilize industry-standard tools, techniques, and methodologies for VAPT activities.

3. **Scope of VAPT:**
- Define the scope and boundaries of systems, networks, and applications to be included in VAPT activities.
- Include both internal and external infrastructure components in the assessment.
- Consider critical systems, high-risk applications, and sensitive data as priority areas for VAPT.

4. **VAPT Execution:**
- Assign qualified and experienced personnel or external service providers to conduct VAPT activities.
- Follow a systematic approach, including pre-engagement, reconnaissance, vulnerability scanning, exploitation, and reporting.
- Ensure proper coordination and communication with relevant stakeholders during VAPT engagements.

5. **VAPT Reporting:**
- Document and report identified vulnerabilities, weaknesses, and recommended remediation actions.
- Include a risk rating or severity level for each vulnerability based on its potential impact and likelihood of exploitation.
- Provide clear and actionable recommendations for remediation, prioritized based on risk level.

6. **Vulnerability Remediation:**
- Establish processes for promptly addressing and remediating identified vulnerabilities.
- Assign responsibility for remediation actions to appropriate individuals or teams.
- Implement a systematic tracking mechanism to monitor the progress of vulnerability remediation efforts.

7. **Security Hardening:**
- Develop security hardening guidelines and standards for various systems, platforms, and applications.
- Regularly review and update the hardening guidelines to address emerging threats and vulnerabilities.
- Implement security hardening measures based on industry best practices and vendor recommendations.

8. **Configuration Management:**
- Maintain a centralized inventory of hardware and software components with their associated configurations.
- Implement configuration management controls to ensure consistency, integrity, and security of system configurations.
- Regularly review and update configurations based on changing security requirements and industry standards.

9. **Patch Management:**
- Establish a patch management process to address vulnerabilities and apply security patches promptly.
- Regularly monitor and assess available patches and their applicability to the organization's systems and applications.
- Test and deploy patches in a controlled environment to minimize disruptions and ensure compatibility.

10. **Compliance and Auditing:**
- Ensure VAPT activities align with applicable laws, regulations, and industry standards.
- Engage in regular compliance audits to assess the effectiveness of VAPT and hardening measures.
- Maintain proper documentation and evidence of VAPT activities and remediation efforts for audit purposes.