SECURITY POLICY

1. INTRODUCTION

At Autom Mate, security is a cornerstone of our operations. We are dedicated to protecting the confidentiality, integrity, and availability of information assets. This policy outlines our commitment to robust security practices, compliance with industry standards, and the safeguarding of client trust.

2. COMPLIANCE AND CERTIFICATIONS

Autom Mate adheres to globally recognized standards to ensure compliance and security excellence:

- Regulatory Alignment: Autom Mate complies with GDPR, Data Privacy Framework, European Economic Area Data Transfers and other relevant data protection laws.
- Standards and Audits: Adherence to ISO 27001 principles and internal security audits ensures continuous improvement.
- Data Protection Addendum (DPA): Ensures secure processing of personal data in compliance with legal requirements.
- Transparency: Security audit reports (when available) are shared with clients under NDA.

3. RISK MANAGEMENT

A structured approach to risk management enables proactive threat mitigation:

- Risk Assessments: Regular evaluations identify and prioritize risks.
- Mitigation Strategies: Risks are addressed through preventive, detective, and corrective controls.
- Incident Documentation: Root cause analyses are conducted for serious incidents to prevent recurrence.

4. DATA SECURITY

Data is safeguarded through comprehensive protection mechanisms:

- Data Classification: Information is classified into Confidential, Restricted, or Public, ensuring appropriate handling.
- Encryption: AES-256 encryption protects data at rest, while TLS safeguards data in transit.
- Retention and Disposal: Data retention policies ensure secure storage only for as long as needed, followed by secure deletion.

5. CRYPTOGRAPHIC CONTROLS

Autom Mate implements robust encryption practices:

- Encryption Standards: All cryptographic processes comply with NIST SP 800-57 guidelines.
- Key Management: Keys are securely stored, and access is limited, ensuring their confidentiality and integrity.

6. SECURE DEVELOPMENT PRACTICES

Security is embedded in our development lifecycle:

- Secure Coding: OWASP Top Ten guidelines are followed to mitigate vulnerabilities.
- Code Reviews: Automated and manual reviews ensure secure code deployment.
- Environment Segregation: Development, staging, and production environments are isolated.

7. ACCESS CONTROL

Access to systems and data is rigorously controlled:

- Role-Based Access Control (RBAC): Permissions are granted based on job roles, adhering to the principle of least privilege.
- Multi-Factor Authentication (MFA): Critical systems require MFA for enhanced security.
- User Access Reviews: Periodic reviews ensure appropriate access levels.

8. EMPLOYEE AND CONTRACTOR SECURITY

Personnel security is a priority at Autom Mate:

- Security Training: Regular training programs ensure awareness of security policies and evolving threats.
- Offboarding Procedures: Access is revoked promptly upon role change or termination.

9. PHYSICAL SECURITY

Physical security measures protect Autom Mate's facilities and assets:

- Access Restrictions: Only authorized personnel can access sensitive areas.
- Monitoring: Surveillance systems ensure facilities are continuously monitored.
- Visitor Management: Protocols regulate visitor access to secure areas.

10. INCIDENT RESPONSE

A structured approach ensures swift handling of security incidents:

- Reporting Mechanism: Incidents are reported through designated channels for immediate action.
- Incident Triage: Issues are categorized by severity and addressed accordingly.
- Post-Incident Reviews: Documentation of lessons learned helps improve response strategies.

11. BUSINESS CONTINUITY AND DISASTER RECOVERY

Autom Mate ensures operational resilience:

- Continuity Plans: Measures like cloud-based redundancy and failover mechanisms guarantee high availability.
- Disaster Recovery Testing: Annual tests validate the effectiveness of recovery protocols.
- Remote Operations: Policies support seamless remote work during emergencies.

12. LOGGING AND MONITORING

Logging and monitoring ensure accountability and early threat detection:

- Activity Logging: System activity is logged, including logins, data access, and configuration changes.
- Real-Time Monitoring: Automated systems detect and alert on unauthorized access attempts.

13. THIRD-PARTY MANAGEMENT

Vendors and service providers are held to high security standards:

- Vendor Assessments: Risk assessments are conducted before engaging third parties.
- Contractual Obligations: Agreements include robust security requirements.
- Ongoing Compliance Monitoring: Vendors are regularly audited for compliance.

14. POLICY GOVERNANCE

Autom Mate’s security policies are governed by structured oversight:

- Policy Owner: The CTO oversees policy implementation and compliance.
- Annual Reviews: Policies are reviewed and updated yearly to address emerging threats.
- Employee Acknowledgment: Personnel are required to acknowledge and adhere to these policies.

15. CONTINUOUS IMPROVEMENT

Autom Mate is committed to evolving its security practices:

- Proactive Measures: Threat intelligence is used to predict and prevent potential risks.
- Feedback Integration: Audit results and user feedback drive enhancements to security measures.

16. TRANSPARENCY AND TRUST

Autom Mate maintains transparency with its clients:

- System Status: Service status and updates are shared in real-time via designated platforms.
- Audit Reports: Available upon request, subject to NDA.

Autom Mate's security policy reflects our commitment to protecting client data and delivering reliable services. Through rigorous controls, continuous improvement, and adherence to global standards, we ensure a secure environment for all stakeholders. For further inquiries, please contact our Data Privacy Officer at dpo@autommate.com.