**TDA Research, Inc.**

**Technical and Organizational Measures (TOMs) for Data Security**

1. Introduction

Purpose: This document outlines the technical and organizational measures implemented by TDA Research to ensure the security and integrity of personal data, in compliance with applicable data protection laws and regulations.

Scope: The measures described apply to all processing activities involving personal data collected, stored, or transmitted by TDA Research, covering all departments and systems handling such data.

Definitions and Acronyms: Terms such as "personal data," "processing," and "data subject" are used as defined in relevant data protection legislation.

2. Risk Assessment

Risk Identification: TDA has ongoing procedures and efforts to identify potential risks include unauthorized access, data breaches, data loss, and system failures that could compromise the confidentiality, integrity, or availability of personal data.

Risk Analysis: Each identified risk is evaluated based on likelihood and potential impact, prioritizing risks that could result in significant harm or legal non-compliance.

Risk Mitigation: Controls are implemented to mitigate risks, including access restrictions, encryption, regular backups, and employee training.

3. Organizational Measures

Data Protection Policies: TDA Research has established data protection policies, including a Privacy Policy and Data Handling Guidelines, which are regularly reviewed and updated.

Roles and Responsibilities: A Data Protection Officer oversees compliance efforts, while all employees are responsible for adhering to data protection policies.

Training and Awareness: Employees receive mandatory data protection training upon hire and annually thereafter, covering best practices and regulatory requirements.

Incident Response Procedures: An incident response plan outlines steps for detecting, reporting, and responding to security incidents, including notification procedures.

Vendor and Third-Party Management: Third-party service providers are assessed for data security practices, and contracts include data protection clauses.

4. Technical Measures

Access Control: Multi-factor authentication is used for system access, with role-based permissions ensuring users have access only to necessary data. Procedures are in place for adding, modifying, and revoking user access, with periodic reviews. Strong password requirements are enforced, with regular mandatory changes and secure storage.

Data Encryption: All data transmitted over networks is encrypted using protocols such as TLS. Sensitive data stored on servers and databases is encrypted using industry-standard algorithms.

Network Security: Firewalls are configured to restrict unauthorized access, and intrusion detection systems monitor for suspicious activities. Network segmentation isolates sensitive systems, reducing risk.

System Security: Systems and applications are regularly updated and patched to protect against vulnerabilities. Antivirus software is installed on all endpoints, with regular updates and scans.

Physical Security: Physical access to facilities is controlled through keycards and biometric systems, with access logs maintained. Data centers have fire suppression systems and climate control.

Backup and Recovery: Regular backups are performed daily, with encrypted copies stored offsite. A disaster recovery plan is in place, with defined recovery time and point objectives.

5. Monitoring and Logging

Event Logging: System and access logs record user activities, access attempts, and system changes. Logs are retained according to policies.

Monitoring Procedures: Continuous monitoring tools detect anomalies, with alerts for critical events.

Audit Trails: Audit logs are reviewed regularly for potential issues, supporting forensic analysis if needed.

6. Data Handling Procedures

Data Minimization: Data collection is limited to what is necessary, employing anonymization or pseudonymization when possible.

Data Retention and Deletion: Data retention schedules are defined, with secure deletion methods when data is no longer needed.

Data Classification: Data is classified based on sensitivity, with handling procedures tailored accordingly.

7. Compliance and Certification

Legal and Regulatory Compliance: TDA Research complies with applicable laws such as GDPR, conducting regular compliance assessments.

Certifications and Standards: The company maintains ISO 27001 certification, adhering to industry best practices.

8. Review and Improvement

Continuous Improvement: Security measures are regularly reviewed and updated in response to new threats or changes in regulations.

Internal Audits: Periodic internal audits assess compliance with policies, with findings addressed promptly.

Document Revision History

Version: 1.0

Date: 2024-12-18

Author: John Wright, Chief Technology Officer

Email: jwright@tda.com

Changes Made: Initial document creation.