Privacy Policy

1. Introduction

Titan (“we,” “our,” or “us”) is committed to protecting the privacy, security, and confidentiality of personal information entrusted to us by our clients. This Privacy Policy describes our data handling practices for our services.

We operate exclusively within the United States and its territories. We do not store, process, or transmit client data outside the United States, and all critical services and sub processors are located in the U.S.

By using our services, you acknowledge and consent to the data practices described in this Privacy Policy.

2. Information We Collect

We collect the following categories of information while providing our services:

2.1 Personal Information - Contact information: Name, business title, email address, phone number, and mailing address - Account credentials: Usernames, passwords, and account preferences - Service usage: Access logs, transaction history, and user activity

2.2 Technical Information - IP addresses, browser type/version, and device identifiers - Application logs and metadata - Cookies and usage analytics data

2.3 Sensitive Personal Information - Financial account details (only as required for service) - Government identifiers where required by law or contract - No biometric or health data is collected unless specifically required for the service

2.4 Data from Third Parties - Business partners or client institutions - Public records and regulatory sources as required for compliance

We do not sell, lease, or share personal information with third parties for marketing purposes.

3. How We Use Your Information

We use the information collected solely for legitimate business purposes including:

3.1 Service Delivery - Provision and maintenance of SaaS services - Account creation, authentication, and access management - Transaction processing and service analytics

3.2 Security and Compliance - Monitoring for fraud and unauthorized activity - Enforcing our Terms of Service and security policies - Performing risk assessments and regulatory reporting

3.3 Client Communication - Providing notifications about service changes or incidents - Responding to support requests and inquiries - Sending legally required communications

3.4 Legal and Regulatory Obligations - Compliance with applicable banking, privacy, and data protection regulations (e.g., GLBA, CCPA, GDPR as applicable) - Responding to subpoenas, legal processes, and regulatory inquiries

4. How We Share Your Information

We disclose information only under these conditions:

4.1 Service Providers and Sub processors - U.S.-based vendors supporting hosting, payment processing, support, and security services - All sub processors undergo security and compliance reviews - Sub processor list is available upon request

4.2 Legal and Regulatory Requirements - In response to valid legal process or regulatory requests - To protect against fraud, security incidents, or as otherwise required by law

4.3 Business Transfers - In the event of a merger, acquisition, or corporate reorganization, subject to equivalent privacy protections

We do not share client data with third parties for independent marketing purposes.

5. Data Security

We implement administrative, technical, and physical safeguards consistent with industry standards for financial services:

5.1 Security Measures - Data encrypted at rest (AES-256) and in transit (TLS 1.2+) - Multi-factor authentication and role-based access controls - Segregated environments for client data - Annual third-party penetration testing and continuous vulnerability scanning - Employee background checks and mandatory security training - Hosting exclusively in Microsoft Azure U.S. regions with SOC 2 and ISO 27001 certified infrastructure

5.2 Incident Response and Breach Notification - Continuous monitoring for security threats and incidents - Documented incident response plan aligned with NIST and FFIEC guidance - Commitment to notify affected clients and regulators in accordance with applicable law

5.3 Data Retention and Disposal - Data retained only as long as necessary to fulfill contractual and regulatory obligations - Secure data destruction aligned with NIST 800-88 media sanitization standards

6. Your Rights and Choices

6.1 Access and Correction - Request access to or correction of personal data - Obtain a copy of data in a portable format where required by law

6.2 Deletion and Restriction - Request deletion of data where permissible - Restrict or object to processing in certain circumstances and as applicable by law

6.3 Marketing and Communication Preferences - Opt-out of non-essential communications at any time

6.4 Cookies and Tracking - Manage preferences via browser settings or our cookie management tool

7. Contact and Governance

Privacy Officer
Name: Kyle Bridges
Email: kyle@manifoldventures.ai
Phone: 404-702-7393

Compliance and Vendor Risk Inquiries
Email: kyle@manifoldventures.ai

We review this policy annually or upon significant regulatory or operational changes to ensure alignment with banking third-party risk standards.