PRIVACY POLICY AND DATA SECURITY GOVERNANCE STATEMENT

(Strictly Optimized for TikTok Shop US Data Security Review)

Effective Date: October 1, 2025

Operator: Shijiazhuang Yuan Supply Chain Management Service Co., Ltd.

Service Name: Submarine AI (Website: qiantingai.com)

Contact Email: admin369@88.com

SECTION 1: INTRODUCTION AND COMMITMENT TO SECURITY

Welcome to Submarine AI (hereinafter referred to as "the Service"). Shijiazhuang Yuan Supply Chain Management Service Co., Ltd. (hereinafter referred to as "We," "Us," or "Our") is the dedicated operator of the Submarine AI platform. We recognize that in the current digital landscape, data security is the cornerstone of trust for our users, sellers, advertisers, and partners.

Compliance Statement for US Data Security Review:

This Privacy Policy and Data Security Statement is established not only to comply with the *Personal Information Protection Law (PIPL)* but also to strictly align with the **Data Security and Privacy Review (DSPR)** standards mandated by the TikTok Shop US Data Security team.

We acknowledge that protecting "Protected Data" (including US seller and buyer data) is a critical obligation. We have implemented a "Defense-in-Depth" security strategy that integrates organizational management with advanced technical controls to ensure that our operations meet or exceed the expectations of the US market. We affirm that an app cannot launch in the TikTok Shop US App Store without adhering to these rigorous security standards.

SECTION 2: SCOPE AND DEFINITIONS

To ensure transparency during the review process, we define the following terms used in this policy:

"Protected Data": Refers to any confidential information obtained through the TikTok Shop Open API or other service channels, including but not limited to Order Information, Seller Details, Buyer PII (Personally Identifiable Information), Item Data, and Transaction Logs.

"Sensitive Personal Information": Includes financial account numbers, government-issued identification numbers, precise geolocation data, and biometric information.

"Processing": Refers to any operation performed on data, such as collection, recording, storage, adaptation, retrieval, use, disclosure by transmission, or deletion.

"Data Minimization": The principle that we only collect data that is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

SECTION 3: INFORMATION COLLECTION AND MINIMIZATION

We strictly adhere to the principle of **Data Minimization**. We do not collect extraneous data. Our data collection is limited to the specific business purpose of providing AI video generation services.

3.1 Information You Voluntarily Provide

- **Account Registration Data:** To create and manage your account, we collect truthful information including your full legal name, business entity name, contact email, and phone number.
- **Identity Verification (KYC/KYB):** To comply with developer and seller verification requirements, we collect identity documents (e.g., Business License, ID Cards). This is strictly for authentication and is stored in a separate, highly secured database.
- **User-Generated Content (UGC):** We process the images, audio files, video scripts, and text prompts you upload solely for the purpose of generating AI video content.
- **Support Communications:** Any data provided during correspondence with our customer support team for dispute resolution or feedback.

3.2 Information Automatically Collected (Technical Data)

- **Device Information:** Device model, operating system version, browser type, screen resolution, and unique device identifiers (IMEI/MAC address).

-
-

  Network Information: IP address, network type (Wi-Fi/4G/5G), and Internet Service Provider (ISP) details.
-
-

  Security & Audit Logs: We record detailed operation logs, including login timestamps, API access records, and session durations. **Note:** These logs are essential for our **Security Auditing** and **Threat Detection** systems and are retained in compliance with cybersecurity laws.
-

SECTION 4: DATA SECURITY ARCHITECTURE (CRITICAL COMPLIANCE)

This section explicitly addresses the technical requirements of the US Data Security Questionnaire. We have implemented the following enterprise-grade security controls:

4.1 Encryption Standards

We employ state-of-the-art encryption to protect data confidentiality and integrity throughout its lifecycle:

-

  Data at Rest: All Sensitive Personal Information and Protected Data stored in our databases (SQL/NoSQL) and object storage systems are encrypted using **AES-256 (Advanced Encryption Standard with 256-bit keys)** or higher. Encryption keys are managed via a dedicated Key Management Service (KMS) with strict rotation policies (every 90 days).
-
-

  Data in Transit: All data transmission between user devices, our servers, and third-party APIs is protected using **TLS v1.2 (Transport Layer Security)** or higher protocols. We strictly prohibit the use of insecure protocols (e.g., HTTP, SSL v3).
-

4.2 Access Control and Authentication

-

  Least Privilege Principle: Access to Protected Data is restricted to employees who have a legitimate business need ("Need-to-Know"). We review access rights quarterly.
-

- **Multi-Factor Authentication (MFA):** We strictly enforce **MFA** (e.g., Google Authenticator, Hardware Tokens) for all administrator accounts and any remote access (VPN) to our production environment. There are no exceptions.
- **Session Management:** To prevent unauthorized physical access, all employee workstations and critical system terminals are configured to **automatically lock the screen after 15 minutes** of inactivity.
- **Account Hygiene:** We enforce strong password policies (requiring a mix of uppercase, lowercase, numbers, symbols, and minimum length). Default passwords are strictly prohibited.

4.3 Network and Infrastructure Security

- **Network Segmentation:** Our production environment is logically and physically isolated from our development and testing environments. We utilize **DMZ (Demilitarized Zones)** and Virtual Private Clouds (VPC) to restrict network traffic.
- **Intrusion Detection:** We deploy **Network Intrusion Detection Systems (NIDS)** to monitor network traffic for suspicious activity 24/7.
- **Firewalls:** We implement Next-Generation Firewalls (NGFW) and Web Application Firewalls (WAF) to block common web attacks (e.g., SQL Injection, XSS).

4.4 Endpoint and Workplace Security

- **Endpoint Protection:** All company servers and employee workstations are equipped with **Host Intrusion Prevention Systems (HIPS)** and enterprise-grade anti-virus software. Virus definitions are updated daily.
- **Vulnerability Management:** We perform automated vulnerability scans on our infrastructure weekly.

-
-

  Penetration Testing: We engage qualified third-party security experts to conduct **Penetration Testing at least annually**. Reports are documented and remediated immediately.

-

  ### 4.5 Incident Response and Business Continuity

-

  We maintain a documented **Incident Response Plan (IRP)**.

-
-

  We conduct **Security Incident Drills at least annually** to test the effectiveness of our detection, containment, and recovery procedures.

-
-

  In the event of a confirmed data breach affecting US users, we will notify the affected parties and relevant regulatory bodies within the timeframes mandated by applicable laws (e.g., 72 hours).

-

  # SECTION 5: DATA RETENTION AND DELETION

-

  Retention Period: We retain Personal Data only for as long as necessary to fulfill the purposes outlined in this policy or as required by law.

-
-

  Deletion Protocol: Upon termination of services or user request, data is securely deleted or anonymized.

-
-

  Seller Data Specifics: If a TikTok Shop seller disconnects their shop or terminates their relationship with us, we will delete all associated Protected Data from our production systems within **7 days** and from backups within **30 days**. We utilize secure deletion methods (e.g., NIST 800-88 guidelines) to ensure data is unrecoverable.

-

SECTION 6: INTERNATIONAL DATA TRANSFERS

Given the global nature of our service, data may be processed on servers located in China and the United States.

- **Compliance Mechanisms:** We adhere to the *Measures for the Security Assessment of Data Outbound Transfer*. For transfers involving US user data, we implement **Standard Contractual Clauses (SCCs)** and Transfer Impact Assessments (TIAs) to ensure that the recipient maintains a level of data protection equivalent to US standards (including the AES-256 encryption requirement).

SECTION 7: SHARING AND DISCLOSURE

We strictly **do not sell** your personal information. We may share data only under the following limited circumstances:

1. **Service Providers:** We share data with trusted cloud infrastructure providers (e.g., AWS, AliCloud) solely for the purpose of storage and computation. These providers are bound by strict **Data Processing Agreements (DPAs)** and must comply with our security standards.
2.
3. **Legal Compliance:** We may disclose information if compelled by a valid court order, subpoena, or to protect the safety of our users or the public.
4.

SECTION 8: YOUR RIGHTS (US & GLOBAL)

We respect your rights regarding your data. Depending on your jurisdiction (including California, Virginia, etc.), you have the following rights:

- **Right to Access:** Request details about the categories and specific pieces of personal information we have collected.
-
- **Right to Delete:** Request the deletion of your personal information ("Right to be Forgotten").
-

- **Right to Correction:** Request the correction of inaccurate data.
- **Right to Opt-Out:** Opt-out of the "sale" or "sharing" of personal information (though we do not sell data).
- **Non-Discrimination:** We will not discriminate against you for exercising your privacy rights.
- To exercise these rights, please contact our Data Protection Officer at **admin369@88.com**. We will verify your identity before processing the request.

SECTION 9: CHILDREN'S PRIVACY

Our services are not intended for individuals under the age of 18. We do not knowingly collect personal information from minors. If we discover that we have inadvertently collected such information, we will take immediate steps to delete it.

SECTION 10: POLICY UPDATES AND CONTACT

We reserve the right to update this policy to reflect changes in legal requirements or our security infrastructure. Significant changes will be communicated via email or website notice.

If you have questions regarding this policy or the **US Data Security Review**, please contact us:

- **Operator:** Shijiazhuang Yuan Supply Chain Management Service Co., Ltd.
- **Address:** Shijiazhuang, Hebei Province, China.
- **Email:** admin369@88.com

潜艇 AI 隐私政策与数据安全合规声明

(针对美国数据安全审查优化终极版)

生效日期： 2025 年 10 月 1 日

运营主体： 石家庄遇安供应链管理服务有限公司（以下简称“我们”、“潜艇 AI”）

服务名称： 潜艇 AI (网址: qiantingai.com)

客服与合规邮箱： admin369@88.com

第一章：引言与安全承诺

欢迎使用潜艇 AI。我们为全球用户提供领先的 AI 视频生成服务。在当今数字化时代，数据安全是我们赢得用户、卖家、广告商及合作伙伴信任的基石。

美国数据安全审查 (US Data Security Review) 合规声明：

本《隐私政策与数据安全声明》不仅依据《中华人民共和国个人信息保护法》(PIPL) 制定，更严格对标 **TikTok Shop 美国数据安全团队** 发布的 **DSPR (数据安全与隐私审查)** 标准。

我们深知保护“受保护数据”（包括美国卖家和买家数据）是至关重要的义务。为此，我们实施了“纵深防御 (Defense-in-Depth)”的安全策略，融合了严格的组织管理与先进的技术控制，确保我们的运营水平完全满足甚至超越美国市场的期望。我们承诺，在完全满足这些严苛的安全标准之前，绝不在 TikTok Shop 美国应用商店发布应用。

第二章：适用范围与关键定义

为确保审查过程的透明度与清晰度，我们对本政策中使用的术语定义如下：

“受保护数据” (Protected Data)： 指通过 TikTok Shop 开放平台 API 或其他服务渠道获取的任何机密信息，包括但不限于订单信息、卖家详情、买家 PII (个人身份信息)、商品数据及交易日志。

“敏感个人信息”： 包括金融账户号码、政府签发的身份证件号码、精确地理位置数据及生物识别信息。

“处理”： 指对数据进行的任何操作或操作集合，如收集、记录、组织、结构化、存储、改编、检索、查询、使用、传输披露、传播或以其他方式提供。

“数据最小化”： 指我们仅收集与处理目的相关且必要的最小数据量的原则。

第三章：信息收集与最小化原则

我们严格遵循 **数据最小化 (Data Minimization)** 原则。我们绝不收集无关数据，我们的数据收集仅限于提供 AI 视频生成服务这一特定业务目的。

3.1 您主动提供的信息

账户注册数据： 为创建和管理您的账户，我们需要收集您的真实信息，包括法定姓名、企业实体名称、联系邮箱及电话号码。

-

-

身份验证 (KYC/KYB)： 为符合开发者及卖家验证要求，我们会收集身份证明文件（如营业执照、身份证）。此类信息仅用于身份认证，并存储于独立的、高度安全的数据库中。

-

-

用户生成内容 (UGC)： 我们处理您上传的图片、音频文件、视频脚本及文本提示词，仅用于为您生成 AI 视频内容。

-

-

客户服务通信： 您为了解决争议或提供反馈而与我们客服团队 (admin369@88.com) 通信时提供的任何数据。

-

3.2 自动收集的信息（技术数据）

-

设备信息： 设备型号、操作系统版本、浏览器类型、屏幕分辨率及唯一设备标识符 (IMEI/MAC 地址)。

-

-

网络信息：IP 地址、网络类型 (Wi-Fi/4G/5G) 及互联网服务提供商 (ISP) 详情。

-

-

安全与审计日志： 我们记录详细的操作日志，包括登录时间戳、API 访问记录及会话时长。**注意：** 这些日志是我们 **安全审计** 和 **威胁检测** 系统的核心组成部分，并依据《网络安全法》要求进行留存。

-

第四章：数据安全架构（审查核心合规条款）

本章节明确回应"美国数据安全问卷"的具体技术要求。 潜艇 AI 已实施以下企业级安全控制措施：

4.1 加密标准 (Encryption Standards)

我们在数据的全生命周期内采用最先进的加密技术以保护其机密性与完整性：

-

静态数据加密 (Data at Rest)： 所有存储在我们数据库 (SQL/NoSQL) 及对象存储系统中的敏感个人信息及受保护数据，均采用 **AES-256 (256 位高级加密标准)** 或更高强度的算法进行加密。加密密钥通过专用的密钥管理服务 (KMS) 进行管理，并执行严格的轮换策略（每 90 天）。

-
-

传输数据加密 (Data in Transit)： 用户设备、我们的服务器及第三方 API 之间的所有数据传输，均强制使用 **TLS v1.2** 或更高版本的安全协议。我们严禁使用不安全的协议（如 HTTP, SSL v3）。

-

4.2 访问控制与身份认证

最小权限原则： 对受保护数据的访问权仅限于具有合法业务需求（“需知原则”）的员工。我们会每季度审查一次访问权限。

多因素认证 (MFA)： 我们对所有管理员账号以及对生产环境的任何远程访问 (VPN)，严格强制执行 **多因素认证 (MFA)**（如 Google Authenticator, 硬件令牌）。此项无例外。

会话管理： 为防止未经授权的物理访问，所有员工的工作终端及关键系统终端均配置为 **无操作 15 分钟后自动锁屏**。

账户安全： 我们执行强密码策略（要求包含大小写字母、数字、符号且满足最小长度）。严禁使用默认密码。

4.3 网络与基础设施安全

网络隔离： 我们的生产环境与开发、测试环境在逻辑和物理上完全隔离。我们利用 **DMZ (非军事区)** 和 VPC (虚拟私有云) 严格限制网络流量。

入侵检测： 我们部署了 **NIDS (网络入侵检测系统)**，对网络流量进行 7x24 小时的全天候监控，以发现可疑活动。

防火墙： 我们实施了下一代防火墙 (NGFW) 和 Web 应用防火墙 (WAF)，以拦截常见的 Web 攻击（如 SQL 注入、XSS 跨站脚本）。

4.4 端点与办公场所安全

端点防护： 公司所有服务器及员工工作终端均安装了 **HIPS (主机入侵防御系统)** 及企业级防病毒软件。病毒特征库每日自动更新。

漏洞管理： 我们每周对基础设施进行自动化的漏洞扫描。

渗透测试： 我们聘请具备资质的第三方安全专家，**每年至少进行一次渗透测试 (Penetration Testing)**。测试报告将存档并立即对发现的问题进行修复。

4.5 应急响应与业务连续性

我们制定了书面的 **网络安全事件应急预案 (IRP)**。

我们 **每年至少组织一次安全事件应急演练**，以测试检测、遏制及恢复流程的有效性。

一旦发生涉及美国用户的确认数据泄露事件，我们将严格按照相关法律法规规定的时限（如 72 小时内）通知受影响方及相关监管机构。

第五章：数据留存与删除

-

留存期限： 我们仅在实现本政策所述目的所需的时间内，或在法律要求的时间内保留个人数据。

删除协议： 服务终止或用户提出请求后，数据将被安全删除或匿名化处理。

卖家数据特别规定： 如果 TikTok Shop 卖家断开店铺连接或终止与我们的合作关系，我们将确保在 **7 天内** 从生产系统中删除所有相关的受保护数据，并在 **30 天内** 从备份系统中删除。我们采用安全销毁方法（如 NIST 800-88 指南）确保数据不可恢复。

-

第六章：国际数据传输

鉴于服务的全球性，数据可能在中国和美国的服务器上进行处理。

-

合规机制： 我们遵守《数据出境安全评估办法》。对于涉及美国用户数据的传输，我们实施 **标准合同条款 (SCCs)** 及传输影响评估 (TIA)，确保接收方维持与美国标准同等的数据保护水平（包括 AES-256 加密要求）。

第七章：信息的共享与披露

我们严格承诺 **不出售** 您的个人信息。我们仅在以下有限情况下共享数据：

服务提供商： 我们仅出于存储和计算目的与可信赖的云基础设施提供商（如 AWS, 阿里云）共享数据。这些提供商受严格的 **数据处理协议 (DPA)** 约束，必须遵守我们的安全标准。

法律合规： 依据法院传票、行政命令或法律强制要求，或为保护用户及公众安全，我们可能披露信息。

第八章：您的权利（美国及全球用户）

我们尊重您对数据的权利。根据您所在的司法管辖区（包括加利福尼亚州、弗吉尼亚州等），您享有以下权利：

访问权： 要求了解我们收集的个人信息的类别和具体内容。

删除权： 要求删除您的个人信息（“被遗忘权”）。

更正权： 要求更正不准确的数据。

拒绝出售权： 选择退出“出售”或“共享”个人信息（尽管我们不出售数据）。

无歧视权： 我们不会因您行使隐私权而对您进行歧视。

如需行使上述权利，请联系我们的数据保护官：**admin369@88.com**。我们将在验证您的身份后处理请求。

第九章：未成年人保护

本服务不面向 18 岁以下的个人。我们不会故意收集未成年人的个人信息。如果我们发现误收集了此类信息，将立即采取措施予以删除。

第十章：政策更新与联系方式

我们保留根据法律要求或安全基础设施的变化更新本政策的权利。重大变更将通过邮件或网站公告通知。

如果您对本政策或 **美国数据安全审查 (US Data Security Review)** 有任何疑问，请联系我们：

运营主体： 石家庄遇安供应链管理服务有限公司

联系地址： 中国河北省石家庄市

合规/客服邮箱： admin369@88.com