empirium

Empirium Governance and Compliance Framework

Overview. Empirium is a global digital marketplace for critical goods, serving highly regulated industries such as aerospace, defense, transportation, and energy. As a trusted platform facilitating transactions between verified buyers and suppliers worldwide, Empirium is committed to operating within a rigorous governance structure that prioritizes compliance, risk management, platform integrity, and responsible technology use. This document sets forth the policies and systems that govern Empirium's operations and serves as a foundational framework for internal enforcement.

Framework. Empirium's governance framework is rooted in strict adherence to U.S. and allied regulatory regimes, including but not limited to the Export Administration Regulations (EAR), International Traffic in Arms Regulations (ITAR), the Office of Foreign Assets Control (OFAC) sanctions programs, the National Defense Authorization Act (NDAA), and Defense Federal Acquisition Regulation Supplement (DFARS). Entities from restricted countries, such as China, Russia, Iran, and others outlined by these regimes, are categorically barred from accessing Empirium. Platform access is contingent upon Know Your Business (KYB) and Know Your Customer (KYC) processes. Every onboarding business must submit comprehensive firmographic data, including business registration, beneficial ownership, DUNS and CAGE codes, NAICS classification, and operational metrics. This data underpins our compliance-driven access control model, which governs platform eligibility and transaction privileges.

Architecture. Our product onboarding architecture is equally structured to enforce regulatory and economic classification. Empirium leverages a flexible data model where each product category is defined by a unique schema ("product shapes") containing tailored form fields aligned to the product's technical and regulatory profile. Whether a user uploads a drone motor or a metal forming machine, the form fields they encounter are mapped directly to frameworks such as the Commerce Control List (CCL), ECCN classifications, ITAR categories, EAR99, and Harmonized Tariff Schedule Codes (HTSC). This allows Empirium to determine product eligibility, licensing requirements, and buyer eligibility at the moment of listing and to maintain full visibility into the regulatory status of every item on the platform.

Risk Management. From an organizational perspective, Empirium's risk management structure includes technology, counsel, compliance analysts, and software engineers. These teams collaborate to maintain audit trails, evaluate flagged activity, implement continuous policy improvements, and respond to external inquiries. Escalation paths are clearly defined for incidents such as attempted onboarding by restricted entities, listing of controlled items without authorization, or detected suspicious activity indicative of money laundering or diversion.

To enforce these controls, Empirium integrates third-party technologies including Trulioo for identity verification and global KYB/KYC workflows, and utilizes AI to assist in classification, risk scoring, and anomaly detection. All product media uploads, particularly images, are subject to

automated and continuous computer vision analysis. This system determines whether uploaded images are representative of permitted commercial items or restricted goods, such as weapon systems—*Empirium will not allow any firearms or weapons or banned substances of any kind onto the platform.*

This real-time content moderation infrastructure allows Empirium to prevent the listing of non-compliant goods before they surface publicly. Complementary NLP systems analyze textual data such as product descriptions, messages, and metadata for the presence of restricted language, euphemisms, or suspicious patterns. These systems are supplemented by a human-in-the-loop process to resolve ambiguous edge cases.

We maintain a knowledge base of high-risk keywords and image patterns linked to restricted content or misuse scenarios. This base feeds into our AI models to provide contextual analysis and real-time enforcement. All user interactions including media uploads, search behavior, and communication are sampled and monitored within a privacy-compliant structure to identify emerging risks. Actions taken may include listing suppression, account suspension, or escalation to regulatory authorities, depending on severity and nature.

Data Security. Empirium maintains data protection and privacy controls in accordance with global standards. Sensitive business and personal data is encrypted at rest and in transit, with tiered access controls and strict third- party data boundaries. All vendor integrations are vetted for compliance with SOC 2, ISO 27001, and relevant privacy regimes. Data retention is governed by a rolling schedule aligned with regulatory expectations and contractual obligations. When datasets are used for analytics or monetization, all personally identifiable information (PII) and sensitive attributes are anonymized to prevent re-identification.

Transactions. Transaction-level compliance is enforced using multi-layer verification, including pre-transaction screening, sanctions checks, and where applicable, license gating for controlled items. Funds movement is handled through pre-vetted escrow and payment partners PayPal, Stripe, and Escrow.com , who operate under their own AML programs and compliance review frameworks. No transaction may clear without full alignment between buyer, seller, product, and regulatory permissions.

Reviews. Empirium conducts routine reviews of this governance framework to reflect changes in law, partner requirements, and platform evolution. All amendments are documented, versioned, and communicated internally and externally as appropriate. The policy is overseen by the compliance officer with support from the governance working group, composed of leadership from legal, compliance, data, and platform operations.

This framework is designed not only to prevent abuse, but to create a defensible trust architecture that allows Empirium to serve customers with speed, assurance, and security.