



PhoenixX Anti-Money Laundering (AML) & Sanctions Compliance Policy

Document Reference: PHX-AML-1.0



PhoenixX Anti-Money Laundering (AML) & Sanctions Compliance Policy

Document Reference: PHX-AML-1.0

Version: 1.0

Effective Date: 1 November 2025

Governing Law: Swiss Substantive Law

Dispute Resolution: Zurich Arbitration (Swiss Rules)

Issued By: Agency PhoenixX LLC

Domain: PhoenixX.one

Document Classification

This document is a legally binding corporate compliance policy. It defines PhoenixX's AML/CTF and Sanctions framework for global operations, including controls for KYC/KYB/UBO verification, risk assessment, sanctions screening, transaction monitoring, suspicious activity reporting, records retention, and cooperation with competent authorities.

Confidentiality Level: Public Legal Document

Applies To: PhoenixX employees, executives, contractors, subcontractors, partner agencies, suppliers and associated business representatives

Status: Approved by PhoenixX Compliance & Risk Management

1. Purpose and Legal Effect

This Anti-Money Laundering and Sanctions Compliance Policy ("Policy") establishes the binding framework to prevent money laundering, terrorist financing, proliferation financing, corruption-linked transactions, sanctions evasion and related financial crime within PhoenixX operations. This Policy is incorporated by reference into all PhoenixX contracts and forms an enforceable condition of engagement for all covered parties. Violations constitute a material breach subject to immediate enforcement, suspension or termination, financial recovery, investigation and referral to competent authorities.

2. Scope and Applicability

This Policy applies globally to all business activities, including onboarding, vendor management, data services, AI services, compliance operations, procurement and payments. It binds employees, contractors, subcontractors, partner agencies, suppliers and any third parties acting on behalf of PhoenixX. PhoenixX reserves the right to block transactions, freeze payments, restrict access to PhoenixX Systems and terminate engagements where AML or sanctions risk is identified.



+1 307 302 4642
info@phoenixx.one
www.phoenixx.one

2106 House Ave Suite 226
Cheyenne 82001 WY / USA



3. Regulatory Framework

PhoenixX aligns its AML/CTF controls with the Financial Action Task Force (FATF) Recommendations, the U.S. Bank Secrecy Act (BSA) and related FinCEN guidance, EU AML Directives, the Swiss Anti-Money Laundering Act (AMLA) and FINMA circulars, and international sanctions regimes administered by OFAC (U.S.), SECO (Switzerland), the Council of the European Union and the UK OFSI. Where standards conflict, PhoenixX applies the strictest applicable measure.

4. Definitions

Money Laundering is the process of concealing the illicit origin of funds. Terrorist Financing means the provision or collection of funds with the intention that they be used to carry out terrorist acts. Proliferation Financing involves the provision of funds for the proliferation of weapons of mass destruction. Sanctions mean restrictive measures issued by competent authorities (e.g., OFAC, SECO, EU, OFSI) against persons, entities, sectors or countries. UBO refers to the ultimate beneficial owner(s) who ultimately own or control a customer or counterparty. CDD means customer due diligence; EDD means enhanced due diligence.

5. Governance and Responsibilities

PhoenixX Compliance & Risk Management oversees the AML/CTF & Sanctions program, reports to executive leadership, maintains written procedures, and ensures periodic reviews. Business units must implement this Policy and report red flags without delay. PhoenixX may appoint a Money Laundering Reporting Officer (MLRO) function responsible for investigations, SAR/STR preparation and liaison with competent authorities.

6. Risk Assessment

PhoenixX performs risk assessments considering customer type, geography, product/service, delivery channel, transaction profile and data provenance. High-risk factors include shell or front companies, opaque ownership, high-risk jurisdictions identified by FATF, sanctioned or embargoed countries, PEP exposure, cash-intensive arrangements, complex layering or rapid movement of funds. Risk ratings drive the depth of CDD/EDD, monitoring and approval requirements.

7. KYC/KYB/UBO Verification

PhoenixX requires identification and verification of counterparties proportionate to risk. For entities, PhoenixX verifies legal existence, registered office, control structure and UBOs; for individuals, PhoenixX verifies identity and, where applicable, residency and tax status. PhoenixX may request government IDs, corporate registers, beneficial ownership declarations, proof of address, tax identification numbers and bank letters. Refusal to provide information triggers onboarding rejection or service suspension.

8. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)

CDD is conducted for all counterparties before engagement. EDD is required for high-risk cases, including PEPs, adverse media, complex structures, or high-risk geographies. EDD measures may include source-of-funds/source-of-wealth checks, independent corporate filings, onsite/remote interviews, reference letters, expanded sanctions and watchlist screening, and senior management approval.





9. Sanctions Screening

PhoenixX performs sanctions screening at onboarding and periodically thereafter against authoritative lists, including OFAC SDN and Consolidated Lists, SECO, EU Consolidated Financial Sanctions, UK OFSI, and UN sanctions lists. Screening applies to counterparties, UBOs, directors, key signatories and relevant transactions. Potential matches are escalated for review. Confirmed matches result in immediate rejection, transaction blocking and reporting consistent with applicable law.

10. Transaction Monitoring and Red Flags

PhoenixX monitors for suspicious activity, including unusual payment routing, sudden volume spikes, circular transactions, split invoicing, unexplained credits, third-party payments without economic purpose, and attempts to bypass sanctions screening. Machine-assisted analytics may be used with human oversight. Alerts are investigated promptly and outcomes documented.

11. Suspicious Activity Reporting (SAR/STR)

Where PhoenixX identifies grounds to suspect money laundering, terrorist financing, proliferation financing or sanctions evasion, PhoenixX prepares and files suspicious activity/transaction reports with competent authorities in accordance with applicable law. PhoenixX may also notify clients or partners when legally permissible but may be restricted by tipping-off prohibitions.

12. Recordkeeping and Retention

PhoenixX retains onboarding, CDD/EDD, screening, monitoring and investigation records for at least ten (10) years from the end of the relationship or longer where legal hold applies. Records must be complete, accurate and accessible for audits, investigations and arbitration. Retention aligns with the PhoenixX Privacy Policy and Annex D (Security & Encryption Statement).

13. Training and Awareness

PhoenixX provides role-appropriate AML/CTF and Sanctions training for personnel and requires attestations of completion. Refusal or failure to complete mandatory training constitutes a breach of this Policy.

14. Independent Review and Testing

PhoenixX conducts periodic independent testing of the AML/CTF & Sanctions program to assess effectiveness, control design, and regulatory alignment. Findings are documented and corrective actions tracked to completion.

15. Cooperation with Authorities

PhoenixX cooperates in good faith with competent authorities, including FIUs, FINMA, OFAC, SECO, EU authorities, OFSI and law enforcement, consistent with legal obligations and data protection laws. PhoenixX may preserve and disclose evidence under lawful process and is authorized to impose Legal Hold on relevant records.



16. Data Protection Alignment

PhoenixX processes AML/CTF data in accordance with its Privacy Policy and applicable data protection laws. Where conflicts arise, PhoenixX applies the strictest standard that enables lawful AML/CTF enforcement. PhoenixX may restrict data subject rights where necessary for crime prevention or legal claims as permitted by law.

17. Enforcement and Consequences

Any breach of this Policy constitutes a material breach. PhoenixX may deny onboarding, suspend services, block or freeze payments, terminate contracts, blacklist entities, retain funds as permitted by law, and pursue arbitration or legal action. Responsible parties shall indemnify PhoenixX for losses, penalties, fines, legal fees and investigation costs arising from their breach.

18. Policy Supremacy and Modification

This Policy prevails over conflicting external AML or sanctions policies tendered by counterparties. PhoenixX may update this Policy at any time. Continued engagement constitutes acceptance of the latest version.

19. Governing Law and Arbitration

This Policy is governed exclusively by Swiss substantive law. Any dispute shall be resolved by final and binding arbitration administered by the Swiss Arbitration Centre under the Swiss Rules, with seat in Zurich, language English. PhoenixX may seek emergency relief, evidence preservation orders and cross-border enforcement. The prevailing party is entitled to recover reasonable legal and arbitration costs.

Annex A – AML/CTF Red Flags (Illustrative)

Category	Examples
----------	----------

Ownership	Unclear UBOs, nominee shareholders, bearer shares
-----------	---

Geography	High-risk or sanctioned jurisdictions (FATF lists)
-----------	--

Transactions	Third-party payments, circular flows, split invoices, excessive refunds
--------------	---

Behavior	Refusal to provide documents, inconsistent information, pressure for urgency
----------	--

Annex B – Sanctions Controls Summary

Screen against OFAC SDN and Consolidated Lists, EU Consolidated List, UK OFSI, SECO and UN lists at onboarding and periodically. Apply transaction screening where appropriate. Block or reject matches and escalate to Compliance & Risk Management.



Annex C – SAR/STR Escalation Protocol

Identify red flag → freeze or block transaction as needed → notify MLRO → collect evidence and conduct analysis → file SAR/STR with the competent FIU where legally required → impose Legal Hold → document outcomes and remediation.

Approval and Enforcement

Approved by: PhoenixX Compliance & Risk Management

Agency PhoenixX LLC

PhoenixX.one

legal@PhoenixX.one | compliance@PhoenixX.one

© 2025 Agency PhoenixX LLC – A Wyoming Limited Liability Company. All rights reserved.

Governing Law: Swiss Substantive Law | Dispute Resolution: Zurich Arbitration (Swiss Rules)

This policy includes mandatory arbitration and contractual enforcement provisions.



+1 307 302 4642
info@phoenixx.one
www.phoenixx.one

2106 House Ave Suite 226
Cheyenne 82001 WY / USA