PhoenixX
Structure. Compliance. Intelligence.

PhoenixX Risk Enforcement & Account Actions Policy

Document Reference: PHX-REA-1.0

PhoenixX Risk Enforcement & Account Actions Policy

Document Reference: PHX-REA-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 enforcement policy. It defines PhoenixX's authority to take risk-based enforcement actions including account suspension, access restriction, payment freezing, contract termination, evidence preservation and permanent blacklisting of high-risk entities.

Confidentiality Level: Public Legal Document
Applies To: Clients, Users, Employees, Contractors, Suppliers and Subcontractors
Status: Approved by PhoenixX Compliance & Risk Management

1. Legal Authority and Enforcement Scope

This Risk Enforcement & Account Actions Policy ("Policy") establishes PhoenixX's legal authority to protect system integrity, compliance operations, commercial safeguards, AI model security, intellectual property, confidential data and business continuity. This Policy applies globally to all Clients, Users, Suppliers, Subcontractors and other entities interacting with PhoenixX Systems. Enforcement actions may be taken at PhoenixX's sole discretion based on risk.

2. Enforcement Grounds and Trigger Conditions

PhoenixX may take enforcement actions where risk, misconduct or legal exposure exists. Trigger conditions include fraud indicators, abuse, security threats, IP theft, AI system misuse, data exfiltration, model extraction attempts, hidden subcontracting, non-compliance with PhoenixX Policies, sanctions risk, financial crime, illegal content, regulatory risk, contract breach or attempted circumvention of PhoenixX controls.

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

2106 House Ave Suite 226
Cheyenne 82001 WY / USA

3. Types of Enforcement Actions

PhoenixX may impose one or more enforcement measures based on severity of risk, including account suspension, credential revocation, access limitation, feature restriction, data quarantine, IP blocking, payment freeze, contract termination and permanent blacklisting. Enforcement decisions are final and taken at PhoenixX's sole discretion based on security, legal and commercial necessity.

4. Account Suspension and Access Restriction

PhoenixX may suspend accounts temporarily or indefinitely where fraud, security risk, policy breach, abusive behavior, false identity, unauthorized activity, AI misuse, data extraction attempts, system manipulation or compliance risk is detected. Suspension may occur without prior notice. PhoenixX is not required to provide reinstatement and has no obligation to disclose risk intelligence sources.

5. Termination and Permanent Ban Authority

PhoenixX may permanently terminate access to PhoenixX Systems and business relationships in cases of Severe Breach. Severe Breach includes financial crime, derived data theft, IP infringement, reverse engineering, hidden subcontracting, provision of illegal content, multi-account manipulation, sanctions risk and legal obstruction. Enforcement decisions are final. **No appeal is permitted** for permanent bans applied due to security, legal or compliance violations.

6. Payment Freezing and Funds Retention

PhoenixX may freeze, withhold or retain payments where fraud, misrepresentation, sanctions risk, AML review, contractual dispute, security breach or forensic investigation is pending. PhoenixX may retain funds as permitted by law to offset damages or unpaid obligations. Payment hold rights apply to both Clients and Suppliers.

7. Evidence Retention and Legal Hold

PhoenixX may enforce Legal Hold on transaction logs, communication records, annotation data, audit trails, model interaction logs, IP addresses and metadata for compliance investigations, arbitration, litigation or law enforcement cooperation. Legal Hold overrides deletion requests and remains active until release by PhoenixX.

8. Blacklisting and Global Risk Registry

PhoenixX maintains a Global Risk Registry of banned customers, suppliers, subcontractors and associated accounts. Entities may be blacklisted for Severe Breach, fraud, hidden agency chains, collusion, AI abuse, content security violations, criminal exposure or repeated non-compliance. Blacklisting is permanent. PhoenixX may share anonymized threat intelligence with trusted security and compliance partners.

9. AI Misuse and System Abuse Enforcement

PhoenixX prohibits AI misuse including automated abuse, synthetic account generation, coordinated manipulation, adversarial model attacks, prompt injection attacks, model extraction, reverse engineering, automated scraping, unauthorized

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

2106 House Ave Suite 226
Cheyenne 82001 WY / USA

dataset harvesting, content laundering and high-volume bot interference. PhoenixX may deploy automated and human-enforced countermeasures to identify and block hostile AI activity. PhoenixX may permanently ban entities involved in AI misuse.

10. Data Security and Intellectual Property Protection

PhoenixX may enforce immediate access revocation, legal hold and forensic investigation where attempted IP theft, data extraction, trade secret acquisition, system replication or unauthorized data transfer is detected. Derived Data, AI Training Data and PhoenixX System Logic are protected commercial assets. Any unauthorized replication, redistribution, resale or transfer constitutes a Severe Breach.

11. Contract Violations and Fraud Response

PhoenixX may apply enforcement when contract fraud, identity misrepresentation, hidden subcontracting, unlawful invoicing, multi-account evasion, collusion, impersonation or breach of commercial integrity is detected. PhoenixX reserves payment retention rights to offset damages, unpaid obligations, data recovery expenses or forensic investigation costs.

12. Enforcement Notices and Legal Communication

PhoenixX may issue enforcement notices electronically or through PhoenixX Systems. PhoenixX is not obligated to provide advance notice where enforcement protects system integrity, legal compliance or investigatory privilege. Enforcement communications may be limited to protect PhoenixX security protocols.

13. Cooperation with Authorities

PhoenixX may cooperate with law enforcement, financial intelligence units (FIUs), cybercrime divisions, sanctions regulators and arbitration bodies. PhoenixX may share evidence where legally required and may retain data for law enforcement support.

14. Liability Shield and No Damages Clause

PhoenixX shall not be liable for any loss of business, profits, contracts, data or reputation resulting from enforcement actions. Enforcement is a contractual right and security necessity. PhoenixX rejects liability for lawful enforcement taken in good faith based on risk assessment.

15. Arbitration and Enforcement Survival

Disputes under this Policy shall be resolved exclusively by arbitration under Swiss law and the Swiss Rules with seat in Zurich. Enforcement rights remain valid after contract termination. PhoenixX may seek emergency injunctions and evidence preservation orders. Legal and arbitration fees shall be recoverable from the offending party.

Approval and Enforcement

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

2106 House Ave Suite 226
Cheyenne 82001 WY / USA

This Risk Enforcement & Account Actions Policy – PHX-REA-1.0 is binding upon all Clients, Users, Suppliers and Subcontractors. Enforcement is mandatory for PhoenixX security and compliance operations. Violations result in permanent access prohibition.

Approved by: PhoenixX Compliance & Risk Management
Agency PhoenixX LLC
PhoenixX.one
legal@PhoenixX.one | compliance@PhoenixX.one

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