PhoenixX
Structure. Compliance. Intelligence.

PhoenixX Information Security Policy

Document Reference: PHX-ISP-1.0

PhoenixX Information Security Policy

Document Reference: PHX-ISP-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 Information Security Policy (ISP). It defines PhoenixX's mandatory security controls, risk protections, access requirements, encryption standards, security governance model, breach response structure and infrastructure protection rules.

Confidentiality Level: Internal – Security Governance
Applies To: All PhoenixX Employees, Contractors, Suppliers, Subcontractors and System Integrations
Status: Approved by PhoenixX Compliance & Risk Management

1. Purpose and Legal Effect

This Information Security Policy ("Policy") establishes the mandatory security controls, enforcement rights, technical safeguards, and operational procedures required to protect PhoenixX Systems, data assets, AI models, infrastructure and confidential business intelligence against unauthorized access, cyber-attacks, data exfiltration, system abuse, insider threats and hostile actors. This Policy is legally binding and forms part of PhoenixX contractual governance. Compliance with this Policy is a condition of access to PhoenixX Systems and infrastructure.

PhoenixX reserves full authority to enforce security controls, restrict access, suspend accounts, freeze system interaction, initiate security lockdowns and conduct forensic investigations where risk is detected. PhoenixX assumes no liability for damages resulting from security enforcement actions taken in good faith to protect system integrity.

2. Scope and Applicability

This Policy applies to all PhoenixX information assets, networks, communication channels, cloud infrastructure, AI systems, storage environments, endpoint devices and data repositories. It applies to all PhoenixX Employees, Contractors, Subcontractors, Agency Partners, Clients and third-party technology vendors with access to PhoenixX Systems. Access to PhoenixX Systems is a privilege, not a right, and may be restricted or revoked based on security risk.

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

2106 House Ave Suite 226
Cheyenne 82001 WY / USA

PhoenixX enforces a **Zero Trust Security Model**. No user, device, network or process is automatically trusted. Security controls apply equally to internal and external entities and extend to all physical, logical and cloud-hosted environments.

3. Security Governance Framework

PhoenixX implements a layered security governance program incorporating:

- NIST Cybersecurity Framework (CSF)
- NIST SP 800-53 Security Controls
- ISO/IEC 27001:2022 Information Security Standard
- SOC 2 Trust Services Criteria (Security, Availability and Confidentiality)
- GDPR Article 32 Security Requirements
- Swiss FADP Security Obligations

PhoenixX Compliance & Risk Management enforces this Policy, supported by Security Engineering, DevSecOps and Infrastructure Operations teams. Security decisions are risk-based and enforceable without prior notice.

4. Risk Management and Threat Prevention

PhoenixX maintains continuous security risk assessments across systems and partners. Threat intelligence and anomaly detection are applied to detect:

- Unauthorized access or credential compromise
- Privilege escalation attempts
- Data extraction and exfiltration
- API abuse and automation attacks
- Botnets and synthetic traffic
- Malware, ransomware and remote access trojans
- AI adversarial attacks and model extraction

PhoenixX may block IPs, revoke credentials, quarantine workloads, introduce rate limits, trigger MFA revalidation and isolate compromised systems.

5. Access Control and Authentication Requirements

Identity access is enforced using:

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

2106 House Ave Suite 226
Cheyenne 82001 WY / USA

- Multi-Factor Authentication (MFA)
- Role-Based Access Control (RBAC)
- Least Privilege Enforcement
- Device Fingerprinting
- Session Monitoring and Timeout Controls
- Continuous Authentication Challenges

Shared accounts, credential reuse, anonymous access, proxy identity use and unauthorized VPN tunneling are strictly prohibited. PhoenixX may require re-identification at any time.

6. Shared Security Responsibility Statement

PhoenixX enforces a Shared Security Model. PhoenixX secures its platforms and core infrastructure; Clients and Suppliers are responsible for securing their own devices, accounts, local networks and data handling practices. PhoenixX is **not liable** for security incidents arising from:

- Unsecured contractor devices
- Malware on supplier or client systems
- Credential sharing or weak passwords
- Unauthorized third-party access
- Local data exports or misconfigured environments
- Insecure public Wi-Fi use or VPN bypassing

Failure by any party to maintain proper security hygiene constitutes a policy violation.

7. Data Protection and Encryption Standards

PhoenixX enforces mandatory encryption requirements. All data in transit must use TLS 1.3 or higher. All data at rest must be encrypted using AES-256 or equivalent cryptographic strength. Encryption keys must be securely stored and rotated. Unauthorized storage of PhoenixX Data outside approved encrypted environments is prohibited. Data localization and access are restricted by jurisdictional compliance.

8. System Monitoring and Forensic Logging

PhoenixX maintains continuous monitoring of access events, privilege escalations, API interactions, security anomalies, automation behavior, model access patterns and data movement. PhoenixX preserves system logs for forensic analysis and

legal evidence in accordance with PHX-DREP-1.0. PhoenixX may conduct covert system security monitoring to detect concealed threats.

9. Security Incident Response Authority

PhoenixX retains authority to immediately respond to suspected or confirmed security threats, including forced credential resets, access lockdowns, IP blocking, system containment, traffic filtering and full infrastructure isolation. PhoenixX may activate Emergency Security Mode and suspend affected accounts without prior notice. PhoenixX is not liable for any disruption caused by defensive security measures.

10. Third-Party Security and Supplier Compliance

All third-party vendors, developers, contractors, IT providers and subcontractors must comply with PhoenixX security controls. PhoenixX may audit third-party environments and revoke access for non-compliance. Use of insecure offshore development vendors or unmanaged third-party resources is prohibited. Only PhoenixX-approved secure development channels may be used.

11. Cloud Security and Infrastructure Resilience

PhoenixX implements security hardening and layered protection including VPC segmentation, firewall enforcement, intrusion prevention, anomaly-based threat detection, backup integrity verification and disaster recovery protocols. PhoenixX maintains georedundancy and controlled failover mechanisms but does not guarantee uninterrupted availability.

12. Secure Development and AI Security Controls

Secure development lifecycle (SDLC) principles apply to all PhoenixX code, pipelines and AI systems. Source code must be version-controlled with access restrictions. AI models and training pipelines are protected from extraction, poisoning, unauthorized fine-tuning and adversarial abuse. All AI deployments must include inference monitoring and security fallback mechanisms.

13. Endpoint and Device Security

Access to PhoenixX Systems is permitted only from security-compliant devices. Personal devices must meet PhoenixX security requirements including full disk encryption, updated operating systems, secure lockscreen, antivirus protection and device identity registration. Use of public or untrusted devices is prohibited. PhoenixX may block device access based on risk signals.

14. Data Transfer and External Storage Restrictions

PhoenixX prohibits the transfer of PhoenixX Data outside approved systems. Unauthorized use of personal storage, USB devices, cloud drives (e.g., Google Drive, Dropbox), messaging apps (e.g., Telegram, WhatsApp), email forwarding or unapproved AI tools for processing PhoenixX Data is forbidden. Shadow IT practices are classified as Severe Breach.

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

2106 House Ave Suite 226
Cheyenne 82001 WY / USA

15. Breach Notification Protocol

PhoenixX shall notify affected parties without undue delay following confirmed detection of a security breach impacting Personal Data or PhoenixX Systems. PhoenixX retains authority to delay notification if immediate disclosure poses a security risk or interferes with an active investigation. PhoenixX complies with GDPR Article 33, Swiss FADP Article 24 and applicable breach reporting requirements.

16. Security Audit and Compliance Monitoring

PhoenixX may conduct compliance reviews, risk audits and security verification on any entity accessing PhoenixX Systems. Third-party suppliers and integrations are subject to periodic security assessments. PhoenixX may require remediation activities, revoke access or terminate relationships based on audit outcomes.

17. Liability Limitation and Security Disclaimer

PhoenixX shall not be liable for losses arising from security incidents caused by Client or Supplier negligence, insecure device practices, credential misuse, unauthorized third-party access or violation of this Policy. Security enforcement actions taken by PhoenixX in good faith are exempt from liability.

18. Governing Law and Arbitration

This Policy is governed by Swiss substantive law. Disputes arising from this Policy shall be resolved exclusively by binding arbitration under the Swiss Rules with seat in Zurich. PhoenixX may seek emergency injunctions, enforcement orders and digital evidence preservation. Arbitration costs are recoverable from the offending party.

Approval and Enforcement

This Information Security Policy – PHX-ISP-1.0 is binding upon all Clients, Users, Employees, Contractors, Suppliers and Subcontractors. Violation of this Policy results in immediate enforcement action.

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)