PhoenixX
Structure. Compliance. Intelligence.

PhoenixX Incident Response & Data Breach Notification Policy

Document Reference: PHX-IRP-1.0

PhoenixX Incident Response & Data Breach Notification Policy

Document Reference: PHX-IRP-1.0
Version: 1.0
Effective Date: 22 July 2025
Governing Law: Swiss Substantive Law
Dispute Resolution: Zurich Arbitration (Swiss Rules)
Issued By: Agency PhoenixX LLC
Domains Covered: PhoenixX.one and PhoenixX Systems

Document Classification

This document is a legally binding Incident Response & Data Breach Notification Policy. It defines breach handling, investigation, legal escalation, and emergency enforcement procedures.

Confidentiality Level: Internal – Security Governance
Applies To: PhoenixX employees, contractors, suppliers, platform operators and partners
Status: Approved by PhoenixX Compliance & Risk Management

1. Purpose and Legal Effect

This Policy establishes PhoenixX's structured process for identifying, reporting, investigating and responding to security incidents and Personal Data breaches. It satisfies GDPR Articles 33–34, Swiss FADP breach obligations and international security requirements. This Policy is legally enforceable and forms part of PhoenixX's contractual compliance framework.

2. Scope and Applicability

This Policy applies to all PhoenixX Systems, infrastructure, cloud services, data environments, AI pipelines and digital communication channels. It applies to employees, contractors, subcontractors, suppliers and any third-party with authorized access. Unauthorized incident handling or suppression of breach evidence is prohibited.

3. Definition of Security Incidents

A Security Incident is any event that compromises, or has the potential to compromise, the confidentiality, integrity or availability of PhoenixX Systems or Data. Incidents include unauthorized access, malware intrusion, data exfiltration, credential abuse, unauthorized privilege escalation, ransomware, service disruption, insider misuse, third-party breach exposure and operational system failure.

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

2106 House Ave Suite 226
Cheyenne 82001 WY / USA

Security Incidents also include **AI Security Incidents**, such as model exploitation, prompt injection attacks, jailbreak manipulation, harmful or unauthorized AI output, model inversion, synthetic identity injection or attempts to extract PhoenixX AI model weights or datasets.

4. Incident Response Authority

PhoenixX retains full authority to initiate emergency enforcement actions to protect its systems during an incident. PhoenixX may:

- Suspend or limit system access
- Freeze accounts or credentials
- Block network routes and API access
- Quarantine affected infrastructure
- Invoke Legal Hold and preserve evidence
- Conduct forensic data acquisition
- Suspend supplier or third-party access

5. Incident Classification Levels

PhoenixX classifies incidents based on severity:

- **Level 1 – Low Severity:** No data impact, minor service event
- **Level 2 – Moderate Severity:** Potential data exposure or service disruption
- **Level 3 – High Severity:** Confirmed intrusion, data impact, security compromise
- **Level 4 – Critical Event:** Major breach, AI data leak, threat actor exploitation, system failure

Classification determines response urgency, escalation and regulatory reporting requirements.

6. Incident Reporting Requirements

All PhoenixX personnel and suppliers must report suspected incidents **immediately** to security@PhoenixX.one. Failure to report known incidents is a breach of contract. External parties must not suppress or bypass incident reporting requirements.

7. Evidence Preservation & Legal Hold

PhoenixX will preserve all relevant incident logs, access records, system telemetry, communication records and forensic data. Legal Hold under PHX-DREP-1.0 applies automatically to all active investigations. Evidence tampering or deletion is strictly prohibited.

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

2106 House Ave Suite 226
Cheyenne 82001 WY / USA

8. Incident Response Team (IRT)

PhoenixX maintains an Incident Response Team responsible for breach coordination, escalation, containment and forensic oversight. The IRT includes representatives from Security Engineering, Infrastructure, Compliance, Legal and Executive functions.

9. Forensic Investigation Procedures

PhoenixX conducts structured forensic investigations to determine incident origin, attack vector, impact scope and responsible parties. PhoenixX may isolate affected assets, duplicate logs, collect forensic images and analyze network telemetry. Cooperation from suppliers and partners is mandatory.

10. Containment Strategy

Containment actions may include isolation of compromised nodes, traffic filtering, credential resets, firewall policy reinforcement, session invalidation, API rate limiting or temporary access suspension.

11. Eradication and Recovery

Upon threat neutralization, PhoenixX will remove malicious artifacts, revoke compromised credentials, resecure systems and restore validated backups. Systems return to service only after security validation.

12. Supplier and Third-Party Breach Protocol

Suppliers must notify PhoenixX of security incidents within 24 hours of detection. Suppliers are fully liable for breaches originating from their systems, staff or subcontractors (IRP-LIAB3). PhoenixX may suspend or terminate supplier access pending investigation and may recover damages under PHX-SSC-1.0.

13. Breach Notification Requirements

PhoenixX complies with GDPR Article 33 and Swiss FADP breach notification requirements. Notification will be made **only when legally required** and based on risk to affected individuals (BN3). PhoenixX will notify the competent authority within 72 hours **when a breach is legally reportable**. PhoenixX may delay notification where necessary to prevent criminal interference or protect system integrity.

14. Communication and Confidentiality

All breach-related communication is controlled by PhoenixX Compliance & Legal. Unauthorized disclosure of breach information is prohibited. Public statements may only be issued by PhoenixX Executive or Legal teams. PhoenixX may withhold certain breach details to protect investigation integrity.

15. Enforcement and Arbitration

This Policy is legally enforceable. PhoenixX may suspend or terminate access to PhoenixX Systems for failure to comply with this Policy. Disputes arising from breach investigation, liability or compliance enforcement shall be resolved by arbitration in Zurich under the Swiss Rules.

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

2106 House Ave Suite 226
Cheyenne 82001 WY / USA

Approval and Enforcement

This Incident Response & Data Breach Notification Policy – PHX-IRP-1.0 is binding across all PhoenixX operations and supply chains. Failure to comply constitutes a material breach and may trigger enforcement under PHX-REA-1.0 (Risk Enforcement & Account Actions Policy) and PHX-SSC-1.0 (Supplier & Subcontractor Compliance Agreement).

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)