# Incident Response Plan

This document outlines PHOCIS Tech's incident response procedures for detecting, containing, eradicating, and recovering from security incidents. Our IRP is modeled on NIST SP 800-61r2 and aligned with GLBA Safeguards Rule breach notification requirements.

## Incident Classification

| Severity | Description | Initial Response SLA |
|---|---|---|
| P1 — Critical | Active breach, data exfiltration, ransomware, system compromise | 15 minutes |
| P2 — High | Unauthorized access, credential compromise, significant data exposure | 1 hour |
| P3 — Medium | Malware detection, policy violation, failed intrusion attempt | 4 hours |
| P4 — Low | Phishing attempt (caught), minor policy issue, anomaly investigation | 24 hours |

## Response Phases

- Preparation — Maintain runbooks, contact lists, and tabletop exercise cadence (quarterly)
- Identification — SIEM alerts, threat intel feeds, and employee reports trigger incident creation in ticketing system
- Containment — Short-term isolation of affected systems; preserve evidence; engage IR retainer if P1/P2
- Eradication — Remove root cause; patch or re-image affected systems; revoke compromised credentials
- Recovery — Restore systems from clean backups; validate integrity; monitor for recurrence
- Post-Incident Review — Root cause analysis within 5 days; lessons learned documented and actioned

## Breach Notification Obligations

- GLBA Safeguards Rule: Notify FTC within 30 days of discovering a breach affecting 500+ customers
- State notification laws: Most states require notification within 30–72 hours of confirmed breach
- FCRA: Notify consumer reporting agencies of unauthorized access to consumer reports
- Investor notification: Material security incidents disclosed to investors within 30 days per disclosure obligations
- PHOCIS maintains cyber liability insurance with a minimum $2M per-occurrence limit

## IR Team & Contacts

| Role | Responsibility |
|---|---|
| IR Lead (CTO) | Overall coordination; declares severity; owns timeline |

| | |
|---|---|
| Security Engineer | Technical containment, forensics, and eradication |
| General Counsel | Legal obligations, breach notifications, regulatory liaison |
| CEO / Exec Sponsor | Investor communications, major escalations |
| External IR Retainer | P1/P2 forensic support and incident management |

## Testing & Continuous Improvement

- Tabletop exercises conducted quarterly with cross-functional leadership team
- Annual full-scale simulated breach exercise with external IR firm
- IRP reviewed and updated after every P1/P2 incident and at minimum annually