Incident Response SLA Excerpt

Purpose and Scope This excerpt defines severity levels, response timelines, communication protocols, and escalation paths for managed incidents in our services. It aligns with NIST IR standards, ISO 27035, and best practices from leading tech firms like Google and AWS. Applies to security incidents, outages, and breaches impacting client data or systems.

Severity Definitions Incidents are classified based on impact to confidentiality, integrity, availability (CIA triad), business operations, and regulatory obligations:

- **Severity 1 (Critical)**: Widespread outage, major data breach, ransomware encryption, or life-safety threats. Examples: Full system compromise, PHI exposure affecting >500 individuals, or service downtime >4 hours.
- **Severity 2 (High)**: Significant degradation, targeted attack, or compliance violation. Examples: Unauthorized access to sensitive data, partial outage affecting key clients, or vulnerability exploitation with potential escalation.
- **Severity 3 (Medium)**: Localized impact, suspicious activity, or minor non-compliance. Examples: Isolated malware, unusual login patterns, or data leak <100 records.
- **Severity 4 (Low)**: Minimal impact, informational alerts, or resolved anomalies. Examples: Failed login attempts or low-risk vulnerabilities.

Response Timelines Timelines start from incident detection or client report. Measured in business hours for Sev 3-4; 24/7 for Sev 1-2.

| Severity | Acknowledgment | Initial Response | Root Cause Analysis | Resolution Target | Post-Incident Review |
|---|---|---|---|---|---|
| Sev 1 | <15 min | <1 hour | <4 hours | <4 hours | <48 hours |
| Sev 2 | <30 min | <2 hours | <8 hours | <24 hours | <5 business days |
| Sev 3 | <1 hour | <4 hours | <24 hours | <3 business days | <10 business days |
| Sev 4 | <4 hours | <1 business day | <3 business days | <5 business days | Optional |

- Acknowledgment: Automated alert confirmation via email/SMS.
- Initial Response: Triage, containment actions, and status update.
- Root Cause Analysis: Preliminary findings shared; full RCA in PIR.
- Resolution: Restoration to normal operations.
- Extensions: Allowed for complex incidents with client approval; penalties apply if SLAs breached (e.g., service credits per Agreement).

Communication Playbooks Standardized templates ensure timely, clear updates. All comms encrypted and logged.

- **Initial Notification**: Within acknowledgment SLA; includes incident ID, severity, description, impact, and next steps. Channels: Email, client portal, phone for Sev 1-2.
- **Status Updates**: Hourly for Sev 1, every 2 hours for Sev 2, daily for Sev 3-4. Format: Brief summary, actions taken, ETA for resolution.
- **Escalation Alerts**: Triggered if timelines slip; notify executives and regulators as required (e.g., GDPR 72-hour breach report).
- **Closure Notification**: Confirms resolution, includes summary RCA, lessons learned, and preventive measures.
- **Regulatory Reporting**: We handle filings (e.g., HIPAA, SEC) with client input; client approves content.
- **Media/External Comms**: Restricted; coordinated via legal team to minimize reputation risk.

Escalation Matrix Escalations ensure rapid resolution. Contact via dedicated IR hotline or portal.

| Level | Trigger | Responsible Party | Contacts | Actions |
|---|---|---|---|---|
| Level 1: Operational | Initial triage; no escalation needed | IR Team Lead | security@thedataexperts.us; On-call rotation | Contain, investigate, update client. |
| Level 2: Management | Timeline slip >50% or increased severity | Security Manager | +1-XXX-XXX-XXXX; legal@thedataexperts.us | Resource allocation, client briefing, RCA acceleration. |

| | | | | |
|---|---|---|---|---|
| Level 3: Executive | Major impact, regulatory involvement, or unresolved > target | CISO/CEO | Executive hotline; Client executive counterpart | Strategic decisions, external experts engagement, crisis PR. |
| Level 4: Board/Regulatory | Catastrophic breach or legal mandates | Board Liaison | As per Agreement | Full disclosure, audits, compliance filings. |

- Client Escalation: Clients may escalate via portal; we respond within 1 hour.
- Testing: Quarterly IR drills simulate scenarios; results shared with clients under NDA.
- Continuous Improvement: Metrics (MTTD/MTTR) tracked; annual playbook reviews incorporate threat intel from sources like MITRE and CrowdStrike.

Contact IR Hotline: ir@thedataexperts.us or +1-XXX-XXX-XXXX (24/7) For customizations, reference the full SLA in your Agreement.