Incident Response Policy

PeopleMetrics, Inc. · April 2026 · External Version

This document is approved for sharing with clients, prospects, and vendors as part of security due diligence requests. It does not contain internal operational details. All content is proprietary and confidential to PeopleMetrics, Inc.

1. Purpose

This policy defines PeopleMetrics' approach to detecting, responding to, and recovering from information security incidents. It applies to all employees, contractors, and third parties who use or manage PeopleMetrics information assets.

2. Incident Classification

Incidents are classified by severity to ensure proportionate and timely response:

- **Low::** Minor impact with no data breach (e.g., blocked spam or failed login attempt).
- **Medium::** Moderate impact with limited or potential data exposure (e.g., unauthorized access attempt).
- **High::** Significant impact involving a major data breach, system outage, or active attack (e.g., ransomware, confirmed data exfiltration).

3. Response Time Objectives

Severity	Response Time Objective	Containment / Resolution Objective
Low	Within 24 hours	Within 72 hours or next business day
Medium	Within 8 hours	Within 24 hours
High	Within 1 hour	Within 4 hours or as soon as possible

4. Incident Response Process

All security incidents follow a structured seven-step response process:

1. **Detection and Reporting::** Incidents are detected through automated monitoring tools and employee reporting. All employees are required to report suspected incidents to the Incident Response Team immediately.
2. **Containment::** Affected systems are isolated to prevent further damage while investigation continues.
3. **Investigation::** Root cause is determined, evidence is collected, and the scope of impact is assessed, including whether client data is affected.

4. **Client Notification Decision::** If client data is involved or suspected to be involved, a formal notification decision is made in accordance with contractual and regulatory obligations. All notification decisions are documented and approved.
5. **Eradication::** The threat is removed and affected systems are secured.
6. **Recovery::** Systems are restored to normal operations and monitored for recurrence.
7. **Post-Incident Review::** Root causes and contributing factors are documented, and policies and controls are updated where necessary to prevent recurrence.

5. Client Notification

PeopleMetrics has a defined client notification program for incidents involving client data. Notification timelines are severity-based and align with contractual and regulatory obligations. Where multiple timelines apply, the most stringent requirement takes precedence:

- **High severity::** Notification within 4 hours of confirmation or reasonable suspicion.
- **Medium severity::** Notification within 12 hours.
- **Low severity::** Notification within 24 hours.

All client notifications are reviewed and approved by the Information Security Officer and CEO prior to delivery. Notifications include a description of the incident, type of data affected, actions taken, and contact details for follow-up.

6. Continuous Improvement

After each incident, the Incident Response Team conducts a formal review to identify root causes, assess control adequacy, define corrective actions, and update policies and training as needed. Incident-derived risks are incorporated into the organization's ongoing risk management program.

7. Regulatory Reporting

Where incidents trigger reporting obligations under applicable laws or regulations (including GDPR and CCPA), PeopleMetrics has predefined escalation channels and contacts in place to fulfill those obligations.

8. Policy Review

This policy is reviewed at least annually and updated following significant incidents or organizational changes.

ISO 27001:2022 Certification · Certificate No. ISMS-PE-092325 · Issued by A-LIGN Compliance and Security, Inc. · Valid through September 23, 2028