Vulnerability Management Policy

PeopleMetrics, Inc. · July 2025 · 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 how PeopleMetrics identifies, evaluates, prioritizes, and remediates vulnerabilities across its systems, applications, and infrastructure to minimize security risk and ensure compliance with ISO/IEC 27001:2022.

2. Scope

This policy applies to all company-managed systems, cloud infrastructure, employee devices, internally developed software, and any third-party services or components used by PeopleMetrics that may impact security.

3. Policy Statement

PeopleMetrics is committed to proactively managing vulnerabilities through regular scanning, tracked remediation, and verification of fixes. All vulnerabilities are addressed according to their risk severity, assessed using industry-standard scoring systems.

4. Vulnerability Management Process

- **Identification::** Automated vulnerability scans are performed on a monthly basis across internal and production environments. Security advisories from vendors and automated dependency monitoring tools are reviewed continuously.
- **Assessment::** Vulnerabilities are assigned a severity rating (Critical, High, Medium, Low) based on industry-standard scoring. The potential impact on systems and data is evaluated for each identified vulnerability.
- **Remediation::** Defined remediation timelines apply based on severity:
  - Critical: within 14 days
  - High: within 30 days
  - Medium/Low: addressed during routine patch cycles or scheduled maintenance
  - Active exploits: emergency patching is applied immediately
- **Verification::** Following remediation, a rescan or manual validation confirms that the vulnerability has been resolved.
- **Exception Handling::** Where a vulnerability cannot be immediately remediated due to business impact, a risk acceptance is formally documented and approved by management.

5. Penetration Testing

PeopleMetrics conducts annual penetration testing of its systems and infrastructure by qualified personnel. Results are reviewed by the Information Security Officer and tracked through to remediation.

6. Reporting and Review

Vulnerability reports are reviewed quarterly by the Information Security Officer. Open vulnerabilities and patch completion status are tracked and maintained as part of the organization's security operations program.

7. Compliance

Compliance with this policy is mandatory. Non-compliance is treated as a security incident and subject to disciplinary action. Adherence is monitored through regular scans, patch reports, and audit reviews.

8. Policy Review

This policy is reviewed at least annually and updated to reflect changes in the threat landscape, technology environment, or regulatory requirements.

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