Information Security Policy

PeopleMetrics, Inc. · May 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

PeopleMetrics is committed to protecting the confidentiality, integrity, and availability of all information it holds on behalf of its clients, respondents, and the organization. This policy establishes the principles and responsibilities governing that commitment.

2. Scope

This policy applies to all employees, contractors, and third parties who access, process, or manage PeopleMetrics information assets. It covers all systems, data, and processes used in the delivery of PeopleMetrics services, including cloud-hosted infrastructure and remote work environments.

3. Information Security Principles

PeopleMetrics manages information security in accordance with the following principles:

- **Least Privilege::** Access to information and systems is granted only to the extent necessary to fulfill a defined role or business purpose.
- **Data Protection by Design::** Security controls are embedded into processes and systems from inception.
- **Risk-Based Approach::** Security measures are proportional to the likelihood and potential impact of identified risks.
- **Continuous Improvement::** Policies and controls are reviewed regularly and updated in response to audit findings, incidents, and changes in the threat landscape.

4. Security Controls

PeopleMetrics maintains and enforces controls across the following domains:

- **Access Control::** Role-based access control (RBAC) and multi-factor authentication (MFA) are enforced across all critical systems. Access rights are reviewed on a regular cadence.
- **Data Security::** Sensitive data is encrypted at rest (AES-256) and in transit (TLS 1.2+). Data is classified by sensitivity, and personal data is anonymized where operationally feasible.
- **Secure Development::** Software development follows secure coding standards, including OWASP Top 10 guidelines. Production data is never used in development or test environments.
- **Incident Response::** A formal incident response program is in place with defined severity classifications, response time objectives, and client notification obligations. All incidents are logged and reviewed.

- **Business Continuity::** Disaster recovery and business continuity plans are documented, tested regularly, and designed to meet defined recovery time and recovery point objectives.
- **Vulnerability Management::** Regular vulnerability scans and penetration testing are conducted. Remediation timelines are defined by severity.
- **Employee Responsibilities::** All employees and contractors complete security awareness training upon onboarding and annually thereafter.

5. Governance

PeopleMetrics has established a formal Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022, certified by an accredited third-party certification body. The ISMS is overseen by a dedicated Information Security Officer and reviewed annually by senior leadership through a formal management review process.

Roles, responsibilities, and accountability structures are documented and communicated across the organization.

6. Compliance

PeopleMetrics' information security program is designed to comply with applicable regulations and frameworks including ISO/IEC 27001:2022, GDPR, and CCPA. Compliance is validated through annual internal audits and external certification audits conducted by an accredited third-party auditor.

Non-compliance with security policies may result in disciplinary action up to and including termination of employment or contract.

7. Policy Review

This policy is reviewed at least annually by the Information Security Officer and updated as necessary to reflect changes in the organization, regulatory environment, or threat landscape.

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