Vendor Risk Assessment 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

This policy establishes how PeopleMetrics assesses and manages information security risks introduced by third-party vendors, service providers, and their personnel. The objective is to ensure the confidentiality, integrity, and availability of PeopleMetrics information assets when engaging third parties or integrating third-party products or services.

2. Scope

This policy applies to all vendors, including third-party service providers, subcontractors, and partners who process, store, or transmit PeopleMetrics data or have access to PeopleMetrics systems.

3. Vendor Risk Assessment

PeopleMetrics conducts a formal security risk assessment for each vendor before engagement and annually thereafter. Assessments cover:

- **Security Controls Review::** Confirmation that the vendor has appropriate controls to protect PeopleMetrics data.
- **Compliance Verification::** Validation that the vendor adheres to ISO 27001 or other recognized security standards and applicable regulations.
- **Incident Response Capability::** Confirmation that the vendor has a defined process for identifying, reporting, and responding to security incidents.

4. Vendor Security Requirements

All vendors with access to PeopleMetrics systems or data must comply with the following requirements:

- **Data Protection::** Sensitive data must be encrypted in transit and at rest.
- **Access Management::** Access to PeopleMetrics data and systems must be restricted to business necessity.
- **Incident Reporting::** Security incidents affecting PeopleMetrics must be promptly reported.
- **Contractual Obligations::** All vendors must agree to security obligations in their vendor agreements, including data protection and compliance responsibilities.

5. Assessment Frequency

- A security risk assessment is completed **before onboarding** any new vendor who processes, stores, or transmits PeopleMetrics data.

- Assessments are repeated **annually** for all active vendors as part of the ISMS maintenance cycle.
- All assessment evidence is documented, retained, and made available for audit or compliance verification.

6. Ongoing Monitoring

PeopleMetrics maintains an active vendor risk management process. Vendors must remediate any identified security deficiencies within agreed timelines. Identified risks are recorded in the organization's risk management program and monitored until resolved.

7. Enforcement

The Information Security Officer is responsible for overseeing vendor security assessments and enforcing this policy. Non-compliance may result in contract suspension or termination.

8. Policy Review

This policy is reviewed annually and updated to reflect changes in the vendor landscape, regulatory requirements, or organizational risk posture.

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