Access Control Policy

PeopleMetrics, Inc. · March 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 establishes the framework for controlling and managing access to PeopleMetrics information systems, applications, and data. It ensures that access is granted only to authorized individuals based on their roles, responsibilities, and need-to-know, in alignment with ISO/IEC 27001:2022.

2. Scope

This policy applies to all employees, contractors, third-party service providers, and any other individuals who require access to PeopleMetrics systems, applications, or data, including externally provisioned personnel where applicable.

3. Access Control Principles

- **Least Privilege::** Access rights are granted based on the minimum privileges necessary to perform defined job functions.
- **Need-to-Know::** Access to sensitive or confidential information is only granted where necessary to fulfill a role.
- **Role-Based Access Control (RBAC)::** Access is assigned based on the user's role within the organization.
- **Separation of Duties::** Duties are divided to prevent any single individual from having unchecked control over a sensitive process.

4. User Access Management

- **User Registration::** All users must be formally registered and authorized before accessing PeopleMetrics systems.
- **Access Requests::** Formal access requests must be submitted with documented justification, reviewed by the relevant manager, and approved by the Information Security Officer before access is granted.
- **External Personnel::** Access for contractors and supplier personnel must reference an active contractual agreement, define a duration, and confirm that required security onboarding has been completed.
- **Account Termination::** Access rights are promptly revoked when a user leaves the organization, changes roles, or reaches a defined access expiration date.
- **Access Reviews::** User access is reviewed at least annually for standard users. Users with access to sensitive data, production systems, or administrative privileges, including external personnel, are reviewed quarterly.

5. External Personnel Accounts

Where supplier or contractor personnel are granted system access, those accounts must be uniquely identifiable, time-bound, approved by an internal system owner, and granted access strictly on a least-privilege basis. Shared accounts are not

permitted. Privileged access for external personnel requires additional approval and is subject to enhanced monitoring.

6. Authentication and System Access

- Multi-factor authentication (MFA) is required for access to all critical systems and remote access.
- Access to sensitive data is controlled through encryption, secure access protocols, and role-based restrictions.
- All access to critical systems and sensitive data is logged. Logs are reviewed regularly to detect unauthorized activity.

7. Training

All users, including employees, contractors, and supplier personnel, must complete access control and security awareness training before access is granted and on a recurring basis thereafter.

8. Compliance and Review

This policy is reviewed at least annually or whenever significant changes occur to systems or organizational structure. Compliance is mandatory for all employees, contractors, and third parties. Violations may result in disciplinary action including termination of employment or contract.

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