Acceptable Use 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 Acceptable Use Policy (AUP) outlines the rules and guidelines governing the use of PeopleMetrics' information technology assets, networks, data, and resources. Compliance with this policy is essential to ensuring security, legal adherence, and the protection of company and client assets.

2. Scope

This policy applies to all employees, contractors, temporary staff, and third-party vendors, including supplier personnel, who access or use PeopleMetrics IT resources. It covers all company-owned and personally-owned devices used for business purposes, cloud-hosted systems, data storage and transfer platforms, and all software applications utilized by the company.

3. Authorized Use

Users are granted access to company assets solely for legitimate business purposes and must:

- Adhere to all organizational policies, legal requirements, and applicable industry standards.
- Respect intellectual property rights, including software licensing agreements.
- Access only those systems and resources for which they have been explicitly authorized.
- Refrain from downloading files or tools without authorization from designated IT personnel.
- Understand that access is revoked immediately upon termination of employment or contract.
- Be individually accountable for all activity performed using their assigned accounts.

4. Network and Internet Usage

- Users must only access authorized websites, applications, and network resources.
- Downloading unauthorized software is prohibited.
- Use of company networks for illegal activities is strictly forbidden.
- Users must connect to a company-approved VPN prior to accessing company systems remotely.

5. Protection of Company Equipment

Users are responsible for maintaining company devices in good working condition. Devices must be secured with passwords, encryption, and other required security measures. Users must lock or log out of devices when unattended and take appropriate precautions when traveling with company equipment.

6. Data Handling and Security

Users must follow the company's data classification and secure handling procedures. Sensitive data must only be transferred using approved, secure methods. Storing company data on unauthorized personal devices or cloud services is prohibited. Data must be disposed of securely in accordance with the company's retention policies.

7. Reporting Security Issues

Users are required to immediately report any suspected security incidents, unauthorized access to systems or data, or loss or theft of company equipment or credentials to the designated security contact. All incidents are logged and reviewed.

8. Third-Party Vendor Access

Third-party vendors and contractors must use company-provided credentials, access only the systems necessary for their engagement, follow all PeopleMetrics security policies and data protection guidelines, and be subject to periodic access reviews.

9. Monitoring

To ensure compliance, PeopleMetrics monitors security events, logs user activity, and conducts periodic security audits and risk assessments. Security awareness training records are maintained.

10. Enforcement

Violations of this policy may result in disciplinary action including verbal or written warning, temporary suspension of access, termination of employment or contract, or legal action where applicable.

11. Policy Review

This policy is reviewed regularly and updated as needed. Changes are communicated to all relevant stakeholders.

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