Change Management 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 a structured approach to managing changes within PeopleMetrics' systems, infrastructure, and applications. It ensures that all changes are planned, reviewed, approved, tested, and documented in alignment with ISO/IEC 27001:2022, while minimizing risk to security, compliance, and business continuity.

2. Scope

This policy applies to all IT systems, networks, applications, and infrastructure used by PeopleMetrics; all software development and production environments; changes to configurations, security settings, and user access controls; and all changes that affect the Information Security Management System (ISMS), including updates to policies, controls, and risk treatment plans. It applies to all employees, contractors, and third parties responsible for system management.

3. Change Management Principles

- **Risk-Based Approach::** Every change is assessed for potential security impact and business risk before implementation.
- **Standardized Process::** All changes follow a structured, documented workflow covering request, review, approval, testing, and post-implementation review.
- **Security and Compliance::** All changes must adhere to ISO/IEC 27001:2022 security controls and applicable regulatory requirements.
- **Minimal Business Disruption::** Changes are planned and scheduled to avoid unnecessary operational downtime.
- **Accountability and Documentation::** All changes are logged and available for audit review.

4. Types of Changes

Type	Description	Approval Required
Standard Change	Routine, low-risk changes with pre-approved procedures (e.g., minor software patches, OS updates)	No (pre-approved)
Normal Change	Changes requiring review and approval due to potential impact (e.g., database schema changes, software upgrades)	Yes

Type	Description	Approval Required
Emergency Change	Critical changes required to resolve security or service incidents (e.g., zero-day security patches)	Yes (expedited); documented retroactively

5. Change Management Process

1. **Request and Documentation::** All proposed changes are formally documented, including description, impact assessment, risk analysis, and rollback plan.
2. **Review and Risk Assessment::** Changes are evaluated for security, compliance, and business impact. High-risk changes require additional approval.
3. **Approval and Scheduling::** Normal and emergency changes require formal approval from IT leadership. Approved changes are scheduled during defined maintenance windows.
4. **Testing and Implementation::** All changes are tested in a controlled environment before deployment, following security best practices.
5. **Post-Change Review::** A post-implementation evaluation confirms stability. All change details are recorded in a change log for audit purposes.

6. ISMS Changes

Changes affecting the ISMS, including policy updates, modifications to security controls, scope changes, and corrective actions from audit findings, follow the same structured process. All ISMS changes are reviewed and approved by the Information Security Officer and senior management, version-controlled, and communicated to relevant stakeholders. ISMS changes are reviewed during the annual management review for effectiveness.

7. Compliance and Review

All changes must be logged and available for audit. Unauthorized or undocumented changes are prohibited. This policy is reviewed annually to ensure continued alignment with ISO/IEC 27001:2022 and evolving business needs.

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