Business Continuity and Disaster Recovery Plan

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 document outlines PeopleMetrics' approach to ensuring business continuity and IT resilience in the event of system failures, cyber incidents, or other disruptions. The goal is to minimize downtime, protect critical information assets, and ensure continued service delivery to clients.

2. Scope

This plan applies to all critical IT infrastructure and cloud services, business-critical communication systems, remote work enablement capabilities, and all employees and third-party service providers involved in IT operations.

3. Business Continuity Commitments

PeopleMetrics is committed to IT resilience through the following measures:

- Maintaining redundant cloud infrastructure to prevent single points of failure.
- Implementing documented disaster recovery processes for all critical systems.
- Ensuring secure remote work capabilities are available to all employees at all times.
- Conducting regular business continuity tests to validate recovery strategies.

4. Recovery Objectives

PeopleMetrics defines the following recovery objectives for critical systems:

- **Recovery Time Objective (RTO)::** The maximum acceptable downtime for critical systems is 90 minutes.
- **Recovery Point Objective (RPO)::** The maximum acceptable data loss is 24 hours, based on regular encrypted backups.

5. Disaster Recovery Process

In the event of a critical system failure, PeopleMetrics follows a defined recovery process:

1. **Detection::** Security monitoring systems detect and log system disruptions.
2. **Assessment::** Incident severity is classified and appropriate escalation is initiated.
3. **Containment::** Immediate actions are taken to prevent further damage, including isolating affected systems.
4. **Restoration::** Data is restored from backups and system integrity is verified.

5. **Root Cause Analysis::** The cause is investigated and recovery strategies are updated accordingly.
6. **Post-Recovery Review::** Lessons learned are documented and procedures are improved.

6. Testing

PeopleMetrics conducts regular disaster recovery testing including backup restoration tests, failover simulations, remote work readiness tests, and cyberattack response drills. A full disaster recovery test is performed at least annually. All test results are logged, reviewed, and used to drive continuous improvement of recovery procedures.

7. Client Notification

If a system outage or disruption affects external services, affected clients will be notified within 4 hours.

8. Contingency Planning

PeopleMetrics operates as a fully remote, geographically distributed organization. All critical systems and data are cloud-hosted and accessible from any location with secure authenticated access, ensuring resilience against single-location or single-device disruptions. Team members are cross-trained to ensure coverage of critical functions in the event a key individual becomes unavailable.

9. Compliance and Review

This plan is reviewed annually and following any major incident. It is maintained in alignment with ISO/IEC 27001:2022 and business continuity best practices.

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