APPLICATION MONITORING SETUP GUIDE

Summit Digital Solutions, Inc.

Document Version: 2.4

Last Updated: January 9, 2024

Classification: Confidential - Internal Use Only

1. PURPOSE AND SCOPE

1. This Application Monitoring Setup Guide ("Guide") establishes the mandatory procedures and configurations for implementing application monitoring across Summit Digital Solutions, Inc.'s ("Company") Peak Performance Platform and associated enterprise systems.

2. This Guide applies to all Company employees, contractors, and authorized third parties responsible for maintaining, deploying, or managing application monitoring solutions.

2. DEFINITIONS

1. "Monitoring Infrastructure" means the collective hardware, software, and network components utilized to collect, process, and analyze application performance metrics.

2. "Alert Threshold" means predetermined performance metric values that trigger notification protocols.

3. "Peak Performance Platform" means the Company's proprietary digital transformation platform, including all associated microservices and dependencies.

3. MONITORING REQUIREMENTS

1. Mandatory Metrics

- Response time (95th percentile)
- Error rates (by category)
- Transaction throughput
- Resource utilization
- API endpoint availability
- Service dependencies
- Custom business metrics

2. Data Retention

- Real-time metrics: 30 days
- Aggregated metrics: 12 months
- Performance snapshots: 24 months
- Critical incident data: 36 months

4. IMPLEMENTATION PROTOCOLS

1. Agent Deployment

a) Production environments must utilize Company-approved monitoring agents version 4.2 or higher.

b) Agent configurations must be version-controlled in the designated repository.

c) All agent deployments must be documented in the Configuration Management Database (CMDB).

2. Authentication & Authorization

a) Monitoring agents must utilize certificate-based authentication.

b) Access credentials must be rotated every 90 days.

c) All credential changes must be logged and audited.

5. ALERT CONFIGURATION

1. Critical Alerts

- Service availability below 99.9%
- Response time exceeding 500ms
- Error rate above 0.1%
- CPU utilization above 85%
- Memory utilization above 90%

2. Warning Alerts

- Service availability below 99.95%
- Response time exceeding 300ms
- Error rate above 0.05%
- CPU utilization above 75%

- Memory utilization above 80%

6. COMPLIANCE AND SECURITY

1. All monitoring data must be encrypted at rest using AES-256 encryption.

2. Data access must comply with the Company's role-based access control (RBAC) policy.

3. Monitoring infrastructure must undergo security assessment quarterly.

4. All monitoring activities must maintain compliance with:

- SOC 2 Type II requirements
- ISO 27001 standards
- GDPR and CCPA regulations where applicable

7. INCIDENT RESPONSE INTEGRATION

1. The monitoring system shall automatically create incident tickets for:

- Critical alert triggers
- Multiple warning alerts within 15 minutes
- Anomaly detection events
- Security-related alerts

2. Incident correlation must be maintained across:

- Application logs
- Infrastructure metrics
- Security events
- Business impact assessments

8. MAINTENANCE AND UPDATES

1. Scheduled maintenance of monitoring infrastructure must be performed monthly.

2. Agent updates must follow the Company's change management process.

3. Configuration changes require approval from:

- Technical Operations Manager

- Security Team Lead
- Service Owner

9. DISCLAIMER AND PROPRIETARY RIGHTS

1. This Guide contains confidential and proprietary information of Summit Digital Solutions, Inc. and may not be reproduced or disclosed without prior written authorization.

2. The Company reserves the right to modify this Guide at any time. All users are responsible for ensuring compliance with the most current version.

10. EXECUTION AND APPROVAL

This Guide has been reviewed and approved by:

_

Dr. Alexandra Reeves

Chief Executive Officer

_

Michael Chang

Chief Technology Officer

_

Sarah Blackwell

Chief Operating Officer

Date: _

Document Control Number: MON-2024-001

Classification: Confidential

Distribution: Internal Use Only