CLOUD OPERATIONS MANUAL

Summit Digital Solutions, Inc.

Version 2.4 - Last Updated: January 9, 2024

1. INTRODUCTION AND SCOPE

1. This Cloud Operations Manual ("Manual") establishes the operational procedures, security protocols, and governance framework for all cloud-based services and infrastructure maintained by Summit Digital Solutions, Inc. ("Company") in connection with its Peak Performance Platform and related digital transformation solutions.

2. This Manual applies to all employees, contractors, and authorized third parties who access, manage, or maintain the Company's cloud infrastructure and related systems.

2. DEFINITIONS

1. "Cloud Infrastructure" means all Company-operated cloud computing resources, including but not limited to servers, storage, networks, software, and platforms deployed across public, private, and hybrid cloud environments.

2. "Peak Performance Platform" refers to the Company's proprietary digital transformation platform incorporating AI, ML, and IoT capabilities.

3. "Critical Systems" means cloud-based systems designated as essential for maintaining client operations and service delivery.

3. CLOUD ARCHITECTURE AND INFRASTRUCTURE

1. Infrastructure Configuration

- Primary cloud provider: Amazon Web Services (AWS)
- Secondary provider: Microsoft Azure
- Hybrid cloud deployment model utilizing private cloud infrastructure for sensitive data processing
- Geographic distribution across US East, US West, and EU Central regions

2. Resource Management

- Auto-scaling groups configured for all production workloads

- Reserved instances for baseline capacity
- Spot instances for non-critical workloads
- Resource tagging requirements per Section 8.2

4. SECURITY AND ACCESS CONTROL

1. Authentication Requirements

- Multi-factor authentication mandatory for all administrative access
- Role-based access control (RBAC) implementation
- Regular access review cycles (minimum quarterly)
- Privileged access management through AWS Security Hub

2. Network Security

- Virtual private cloud (VPC) segmentation
- Security groups and network ACLs
- Web application firewall (WAF) implementation
- DDoS protection via AWS Shield Advanced

5. OPERATIONAL PROCEDURES

1. Change Management

- All infrastructure changes require documented approval
- Change advisory board review for critical system modifications
- Maintenance windows: Sunday 02:00-06:00 EST
- Rolling updates for zero-downtime deployments

2. Monitoring and Alerting

- 24/7 infrastructure monitoring via CloudWatch
- Alert severity levels and response times:
- Critical: 15-minute response
- High: 1-hour response
- Medium: 4-hour response
- Low: Next business day

6. DISASTER RECOVERY AND BUSINESS CONTINUITY

1. Backup Requirements

- Daily incremental backups
- Weekly full backups
- 30-day retention period
- Cross-region replication for critical data

2. Recovery Objectives

- RTO (Recovery Time Objective): 4 hours for critical systems
- RPO (Recovery Point Objective): 15 minutes for critical systems
- Annual DR testing requirement

7. COMPLIANCE AND AUDIT

1. Compliance Requirements

- SOC 2 Type II controls
- GDPR compliance for EU operations
- CCPA compliance for California data
- Annual third-party security assessments

2. Audit Logging

- CloudTrail enabled across all regions
- Log retention: 365 days
- Automated log analysis and alerting
- Quarterly log review requirements

8. COST MANAGEMENT

1. Budget Controls

- Monthly cloud spend monitoring
- Department-level cost allocation
- Automated cost anomaly detection
- Quarterly cost optimization reviews

2. Resource Tagging

- Mandatory tags: Department, Environment, Project
- Cost center assignment
- Application owner
- Compliance classification

9. VENDOR MANAGEMENT

1. Cloud Service Provider Requirements

- Minimum SLA requirements: 99.95% availability
- Security certification requirements
- Regular vendor performance reviews
- Backup provider arrangements

10. DOCUMENT CONTROL

1. Manual Maintenance

- Annual review requirement
- Quarterly updates as needed
- Change log maintenance
- Version control through GitHub Enterprise

2. Distribution

- Available on Company intranet
- Controlled copy distribution
- Training requirements for new employees
- Annual acknowledgment requirement

APPROVAL AND EXECUTION

This Manual has been reviewed and approved by the undersigned authorized representatives of Summit Digital Solutions, Inc.

Approved by:

Michael Chang

Chief Technology Officer

Date: January 9, 2024

Sarah Blackwell

Chief Operating Officer

Date: January 9, 2024