API GATEWAY CONFIGURATION MANUAL

Summit Digital Solutions, Inc.

Document Version: 2.4

Last Updated: January 9, 2024

Classification: CONFIDENTIAL

1. INTRODUCTION AND SCOPE

1. This API Gateway Configuration Manual ("Manual") sets forth the authorized configuration standards, security protocols, and operational procedures for the Summit Digital Solutions Peak Performance Platform(TM) API Gateway infrastructure.

2. This Manual is a controlled document subject to Summit Digital Solutions' Information Security Management System (ISMS) and shall be reviewed annually by the Chief Technology Officer or their designee.

2. DEFINITIONS

1. "API Gateway" means Summit's proprietary middleware layer that manages, routes, and secures all API traffic between the Peak Performance Platform and client systems.

2. "Production Environment" means the live operating environment serving client traffic.

3. "Staging Environment" means the pre-production testing environment used for validation.

4. "Security Token" means the encrypted authentication credential required for API access.

3. GATEWAY ARCHITECTURE

1. Core Components

- Load Balancer Layer
- Authentication & Authorization Layer
- Request/Response Transform Layer
- Rate Limiting & Throttling Layer
- Analytics & Monitoring Layer
- Cache Layer

2. High Availability Configuration

- Minimum N+1 redundancy across all components
- Geographic distribution across AWS regions us-east-1 and us-west-2
- Automated failover with < 30 second recovery time objective (RTO)

4. SECURITY REQUIREMENTS

1. Authentication Protocols

- OAuth 2.0 with JWT tokens required for all endpoints
- Multi-factor authentication for administrative access
- Certificate-based mutual TLS authentication
- Regular rotation of security credentials

2. Encryption Standards

- TLS 1.3 required for all API communications
- AES-256 encryption for data at rest
- HSM-based key management
- Perfect forward secrecy enabled

5. PERFORMANCE CONFIGURATIONS

1. Rate Limiting

- Default limit: 1000 requests per minute per client
- Burst capacity: 150% of base limit for 60 seconds
- Custom limits available via written agreement

2. Caching Parameters

- Default TTL: 300 seconds
- Maximum cache size: 10GB per instance
- Cache invalidation via API or automatic expiry
- Configurable per-endpoint cache policies

6. MONITORING AND LOGGING

1. Required Metrics

- Request latency (95th percentile)
- Error rates by endpoint
- Authentication failures
- Cache hit/miss ratios
- CPU/memory utilization
- Active connections

2. Log Retention

- Access logs: 90 days online, 7 years archived
- Error logs: 30 days online, 3 years archived
- Security logs: 1 year online, 7 years archived

7. DISASTER RECOVERY

1. Backup Requirements

- Full configuration backup daily
- Transaction logs backed up hourly
- Cross-region replication enabled
- Monthly recovery testing required

2. Recovery Procedures

- Automated failover for component failures
- Manual failover for region-level incidents
- Documentation of all recovery events
- Post-incident analysis required

8. COMPLIANCE AND AUDITING

1. The API Gateway infrastructure shall maintain compliance with:

- SOC 2 Type II
- ISO 27001
- GDPR
- CCPA
- Industry-specific standards as required by client agreements

2. Quarterly security audits shall be performed by qualified third parties.

9. MODIFICATION AND MAINTENANCE

1. Changes to this Manual must be approved by:

- Chief Technology Officer
- Chief Information Security Officer
- Chief Digital Officer

2. Version control shall be maintained in Summit's document management system.

10. LEGAL NOTICES

1. CONFIDENTIALITY: This document contains confidential and proprietary information of Summit Digital Solutions, Inc. Unauthorized reproduction or distribution is prohibited.

2. DISCLAIMER: Summit Digital Solutions makes no warranties, express or implied, regarding the completeness or accuracy of this document.

APPROVAL AND EXECUTION

APPROVED AND ADOPTED this 9th day of January, 2024.

SUMMIT DIGITAL SOLUTIONS, INC.

By: _

Michael Chang

Chief Technology Officer

By: _

James Henderson

Chief Digital Officer